DVTEL INC.
65 Challenger Road
Ridgefield Park, NJ 07660

ioimage HD
CF-5212 and CF-5222
Fixed Analytic IP Camera
User and Installation Guide

Rev A12 December 2014

Table of Contents

List of Figures

1 Document Information

Document Scope and Purpose

The purpose of this document is to provide instructions and installation procedures for physically connecting the ioimage HD CF-5212/CF-5222 fixed analytic IP camera. After completing the physical installation, additional setup and configurations may be required before video analysis and detection can commence. For information on the unit setup and configuration, refer to the *HTML Edition Units User's Guide*.

Note:

This document is intended for use by technical users who have a basic understanding of CCTV camera/video equipment and LAN/WAN network connections.

Remarque:

Ce document est destiné aux utilisateurs techniciens qui possèdent des connaissances de base des équipements vidéo/caméras de télésurveillance et des connexions aux réseaux LAN/WAN.

Warning:

Installation must follow safety, standards, and electrical codes as well as the laws that apply where the units are being installed.

Avertissement:

L'installation doit respecter les consignes de sécurité, les normes et les codes électriques, ainsi que la législation en vigueur sur le lieu d'implantation des unités.

Proprietary Rights and Non-Disclosure

This manual is delivered subject to the following restrictions and conditions:

- This document contains proprietary information belonging to DVTEL, Inc. This information is supplied solely for the purpose of assisting explicitly the licensee of the DVTEL units.
- No part of this document contents may be used for any other purpose, disclosed to any third party or reproduced by any means, electronic or mechanical, without the express prior written permission of DVTEL, Inc.

Trademarks and Copyrights

DVTEL, the DVTEL logo, ioimage, the ioimage logo, ioimage analytics, ioibox, ioicam, ioimage HD, ioimage IP, ioimage Thermal, and Site Viewer are trademarks of DVTEL, Inc. Products and trademarks mentioned herein are for identification purposes only and may be registered trademarks of their respective companies. DVTEL, Inc. makes no representations whatsoever about any other products or trademarks mentioned in the manual.

Disclaimer

Users of DVTEL products accept full responsibility for ensuring the suitability and considering the role of the product detection capabilities and their limitation as they apply to their unique site requirements.

DVTEL, Inc. and its agents make no guarantees or warranties to the suitability for the users' intended use. DVTEL, Inc. accepts no responsibility for improper use or incomplete security and safety measures.

Failure in part or in whole of the installer, owner, or user in any way to follow the prescribed procedures or to heed WARNINGS and CAUTIONS shall absolve DVTEL, Inc. and its agents from any resulting liability.

Specifications and information in this guide are subject to change without notice.

Avis de non-responsabilité

Il incombe aux utilisateurs des produits DVTEL de vérifier que ces produits sont adaptés et d'étudier le rôle des capacités et limites de détection du produit appliqués aux exigences uniques de leur site.

DVTEL, Inc. et ses agents ne garantissent d'aucune façon que les produits sont adaptés à l'usage auquel l'utilisateur les destine. DVTEL, Inc. ne pourra être tenu pour responsable en cas de mauvaise utilisation ou de mise en place de mesures de sécurité insuffisantes.

Le non respect de tout ou partie des procédures recommandées ou des messages d'AVERTISSEMENT ou d'ATTENTION de la part de l'installateur, du propriétaire ou de l'utilisateur dégagera DVTEL, Inc. et ses agents de toute responsabilité en résultant.

Les spécifications et informations contenues dans ce guide sont sujettes à modification sans préavis.

Document Conventions

WARNING and **CAUTION** notes are distributed throughout this document, whenever applicable, to alert you of potentially hazardous situations. These may be hazards associated with a task or a procedure you are carrying out or are about to carry out.

The following document conventions are used throughout this manual:

Conventions relatives au document

*Les remarques **AVERTISSEMENT** et **ATTENTION** sont réparties dans l'ensemble du document, en fonction des besoins, afin de vous avertir des situations potentiellement dangereuses. Il peut s'agir de risques associés à une tâche ou à une procédure que vous effectuez ou êtes sur le point d'effectuer.*

Les conventions suivantes sont utilisées dans l'ensemble du document:

A **Warning** is a precautionary message that indicates a procedure or condition where there are potential hazards of personal injury or death.

***Avertissement** est un message préventif indiquant qu'une procédure ou condition présente un risque potentiel de blessure ou de mort.*

A **Caution** is a precautionary message that indicates a procedure or condition where there are potential hazards of permanent damage to the equipment and or loss of data.

***Attention** est un message préventif indiquant qu'une procédure ou condition présente un risque potentiel de dommages permanents pour l'équipement et/ou de perte de données.*

A **Note** is useful information to prevent problems, help with successful installation, or to provide additional understanding of the products and installation.

*Une **Remarque** est une information utile permettant d'éviter certains problèmes, d'effectuer une installation correcte ou de mieux comprendre les produits et l'installation.*

A **Tip** is information and best practices that are useful or provide some benefit for installation and use of DVTEL products.

*Un **Conseil** correspond à une information et aux bonnes pratiques utiles ou apportant un avantage supplémentaire pour l'installation et l'utilisation des produits DVTEL.*

General Cautions and Warnings

This section contains information that indicates a procedure or condition where there are potential hazards.

SAVE ALL SAFETY AND OPERATING INSTRUCTIONS FOR FUTURE USE.

Although the unit is designed and manufactured in compliance with all applicable safety standards, certain hazards are present during the installation of this equipment.

To help ensure safety and to help reduce risk of injury or damage, observe the following:

Précautions et avertissements d'ordre général

Cette section contient des informations indiquant qu'une procédure ou condition présente des risques potentiels.

***CONSERVEZ TOUTES LES INSTRUCTIONS DE SÉCURITÉ ET D'UTILISATION POUR POUVOIR VOUS Y RÉFÉRER ULTÉRIEUREMENT**.*

Bien que l'unité soit conçue et fabriquée conformément à toutes les normes de sécurité en vigueur, l'installation de cet équipement présente certains risques.

Afin de garantir la sécurité et de réduire les risques de blessure ou de dommages, veuillez respecter les consignes suivantes:

Warning:

1. The unit's cover is an essential part of the product. Do not open or remove it.
2. Never operate the unit without the cover in place. Operating the unit without the cover poses a risk of fire and shock hazards.
3. Do not disassemble the unit or remove screws. There are no user serviceable parts inside the unit.
4. Only qualified trained personnel should service and repair this equipment.
5. Observe local codes and laws and ensure that installation and operation are in accordance with fire, security and safety standards.

Avertissement:

1. *Le cache de l'unité est une partie essentielle du produit. Ne les ouvrez et ne les retirez pas.*
2. *N'utilisez jamais l'unité sans que le cache soit en place. L'utilisation de l'unité sans cache présente un risque d'incendie et de choc électrique.*
3. *Ne démontez pas l'unité et ne retirez pas ses vis. Aucune pièce se trouvant à l'intérieur de l'unité ne nécessite un entretien par l'utilisateur.*
4. *Seul un technicien formé et qualifié est autorisé à entretenir et à réparer cet équipement.*
5. *Respectez les codes et réglementations locaux, et assurez-vous que l'installation et l'utilisation sont conformes aux normes contre l'incendie et de sécurité.*

Caution:

To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit's requirements (cooling/heating). Operating temperature should be kept in the range specified for the product (0° to 50°C/32° to 122°F), with no more than 90% non-condensing humidity.

Attention:

Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la régulation de température est suffisante pour répondre aux exigences de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage de température spécifiée pour le produit (0° à 50°C/32° à 122°F), sans condensation d'humidité supérieur à 95%.

Electrical Safety Notice and Warnings

Warning:

1. Read the installation instructions before you connect the unit to a power source.
2. Electrical safety should always be observed. All electrical connections must be performed by a certified electrician.
3. Use the supplied power supply and protect against static electricity, ground faults and power surges.
4. The unit uses a three-wire power cord to make sure that the product is properly grounded when in use. This is a safety feature. If the intended power outlet does not support three prongs, one of which is a ground, contact an electrician to install the appropriate outlet. NEVER remove or otherwise attempt to bypass the ground pin of the power cord. Do not operate the unit in the absence of a suitably installed ground conductor.
5. If you use an extension cord with this system, make sure that the total ampere rating on the products plugged into the extension cord does not exceed the extension cord ampere rating.
6. To avoid possible shock hazards or damaging the unit, assure that the positive and negative of the power leads are properly connected to the terminal block connector before plugging it into the unit or turning on the power source.
7. In the following situations, the electric power should be turned off immediately and appropriate repairs, replacements or remedies should be taken if:
   - The power line is damaged, frayed or shows heavy wear.
   - The unit has been physically crushed or deformed.
   - The unit has been exposed to water.
   - The unit has been exposed to, or shows signs of damage from, fire, intense heat, heavy smoke, fumes, or vapors.
   - Electrical connections of the unit become abnormally hot or generate smoke.
   - The unit has been dropped, damaged or shows signs of loose internal parts.
   - The unit does not operate properly.

Avis et avertissements relatifs à la sécurité électrique

Avertissement:

1. *Lisez les instructions d'installation avant de brancher l'unité à une source d'alimentation électrique.*
2. *Les consignes de sécurité électrique doivent toujours être respectées. Toutes les connexions électriques doivent être effectuées par un électricien qualifié.*
3. *Utilisez l'alimentation fournie, et protégez l'unité contre l'électricité statique, les défauts de mise à la terre et les surtensions.*
4. *Si l'unité utilise un cordon d'alimentation à trois fils, assurez-vous que le produit est correctement mis à la terre du produit lors de son utilisation. Ne retirez JAMAIS, et ne tentez pas de contourner la broche de mise à la terre du cordon d'alimentation. N'utilisez pas l'unité en l'absence d'un conducteur de mise à la terre installé correctement.*
5. *Si vous utilisez une rallonge avec ce système, assurez-vous que l'ampérage total des produits branchés sur la rallonge ne dépasse pas l'ampérage nominal de celle-ci.*
6. *Pour éviter tout risque de choc électrique ou d'endommager l'unité, assurez-vous que les bornes plus et moins de l'alimentation sont correctement raccordées au connecteur du bloc de jonction avant de le brancher sur l'unité ou d'activer la source d'alimentation.*
7. *Dans les situations suivantes, l'alimentation électrique doit être coupée immédiatement, et les réparations, remplacements ou solutions suivants doivent être effectués si :*
   - *Le cordon d'alimentation ou la prise (le cas échéant) est endommagé, effiloché ou très usé.*
   - *L'unité a subi un choc ou a été déformée.*
   - *L'unité a été exposée à de l'eau.*
   - *L'unité a été exposée à, ou montre des signes de dégâts par le feu, une chaleur intense, une fumée épaisse, des émanations ou des vapeurs.*
   - *Les connexions électriques chauffent de façon anormale ou produisent de la fumée.*
   - *L'unité est tombée, a été endommagée, ou certaines pièces internes semblent détachées.*
   - *L'unité ne fonctionne pas correctement.*

Minimizing EMI and RFI	*Minimisation des IEM et des IRF*
When wires run for a significant distance in an electromagnetic field, electromagnetic interference (EMI) can occur. Strong EMI (e.g. lightning or radio transmitters) can destroy the units and can pose an electrical hazard by conducting power through lines and into the system. Poor quality or worn wiring can result in radio frequency interference (RFI). To minimize the effects of EMI and RFI, consult your reseller.	*Lorsque des câbles parcourent une distance importante dans un champ électromagnétique, des interférences électromagnétiques (IEM) peuvent se produire. D'importantes IEM (comme la foudre ou un émetteur radio) peuvent détruire les unités et présenter un risque électrique si elles se propagent sur les câbles et dans le système. Des câbles de mauvaise qualité ou usés peuvent provoquer des interférences radioélectriques (IRF). Pour minimiser les effets des IEM et des IRF, consultez votre revendeur.*

Site Preparation

There are several requirements that should be properly addressed prior to installation at the site. The following specifications are requirements for proper installation and operation of the unit:

- **Ambient Environment Conditions**: Avoid positioning the unit near heaters or heating system outputs. Avoid exposure to direct sunlight. Use proper maintenance to ensure that the unit is free from dust, dirt, smoke, particles, chemicals, water or water condensation, and exposure to EMI.
- **Accessibility**: The location used should allow easy access to unit connections and cables.
- **Safety**: Cables and electrical cords should be routed in a manner that prevents safety hazards, such as from tripping, wire fraying, overheating, etc. Ensure that nothing rests on the unit's cables or power cords.
- **Ample Air Circulation**: Leave enough space around the unit to allow free air circulation.
- **Cabling Considerations**: Units should be placed in locations that are optimal for the type of video cabling used between the unit and the cameras and external devices. Using a cable longer than the manufacturer's specifications for optimal video signal may result in degradation of color and video parameters.
- **Physical Security**: The unit provides threat detection for physical security systems. In order to ensure that the unit cannot be disabled or tampered with, the system should be installed with security measures regarding physical access by trusted and un-trusted parties.
- **Network Security**: The unit transmits over IP to security personnel for video surveillance. Proper network security measures should be in place to assure networks remain operating and free from malicious interference. The unit is intended for installation on the backbone of a trusted network.
- **Electrostatic Safeguards**: The unit as well as other equipment connected to it (relay outputs, alarm inputs, racks, carpeting, etc.) shall be properly grounded to prevent electrostatic discharge.

The physical installation of the unit is the first phase of making the unit operational in a security plan. The goal is to physically place the unit, connect it to other devices in the system, and to establish network connectivity.

2 Overview

The ioimage HD CF-5212/CF-5222 series fixed cameras feature built-in video analytics.

- The CF-5212 is a 1.3 megapixel, HD 720p device.
- The CF-5222 is a 2.1 megapixel, Full HD 1080p device.

The cameras provide real-time, H.264 and MJPEG streaming video with the highest quality image. Featuring a compact, sophisticated and aesthetic mechanical design, the lightweight CF-5212 and CF-5222 cameras are easy to install and operate.

Caution:

If you are using DVTEL Latitude, we recommend that you configure the camera's settings via the AdminCenter. This is because the camera's web-based interface might be overwritten by Latitude settings. Refer to the Latitude online help for information regarding configuring camera settings.

Attention:

Si vous utilisez DVTel Latitude, nous vous conseillons de configurer les paramètres de la caméra via l'AdminCenter. En effet, l'interface Internet de la caméra peut être remplacée par les paramètres Latitude. Veuillez consulter l'aide en ligne Latitude pour de plus amples informations sur la configuration des paramètres de la caméra.

2.1 Features

Following are key features of the CF-5212/CF-5222 camera system:

- Progressive scan CMOS sensor
- H.264 and MJPEG compression
- Low lux
- Day/Night (IR Cut Filter)
- True multi-exposure Wide Dynamic Range
- 2D/3D noise reduction
- RTSP support
- Analog video output
- BNC analog output
- ONVIF support
- Multiple users
- Supports PoE/12VDC/24VAC
- Security IP restricted access allow/deny list
- Built-in web application/ web server
- SNMP v1/v2/v3 SNMP traps
- HTTP streaming MPEG
- Group permissions
- Per-user permissions
- E-mail SMTP alarm notification (up to two e-mails)
- FTP upload (up to two locations)
- HTTP notification server support
- Detection event-driven alarms
- Alarm input driven events
- Relay output actions on alarm
- Dual HTTP notification server support (up to two servers)
- Upload alarm images to FTP
- Historical motion detection levels detected and recorded at frame levels.
- Sequential snapshot numbering
- UPnP support

The camera supports the following analytic functions:

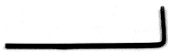
- Analytic relay events
- Reduced false alarm rate
- Increased detection distance

- Intrusion Detection
- Unattended Baggage Detection
- Object Removal Detection
- Stopped Vehicle Detection
- Loitering Detection
- Camera Tampering Detection

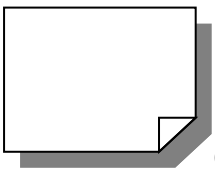
2.2 Package Contents

Before proceeding, check that the box contains the items listed here. If any item is missing or has defects, do not install or operate the product. Contact your dealer for assistance.

Fixed Analytic IP Camera



Back focus adjuster



Quick Installation Guide

CD with bundled software and documentation

Figure 1: Package Contents

Related Documentation

- *ioimage HTML Edition Units User's Guide*
- *ioimage HD CF-5212/CF-5222 Quick Installation Guide*
- *DNA 2.0 User Manual*

3 Introduction to the CF-5212 and CF-5222 Fixed IP Cameras

This chapter provides the camera dimensions for reference before installation. Each connector located inside the camera's housing is also identified. See Figure 3 and Table 1.

The chapter includes the following topics:

3.1 CF-5212/CF-5222 Camera Dimensions

The mechanical dimensions of a CF-5212/CF-5222 Fixed IP Camera are shown below.

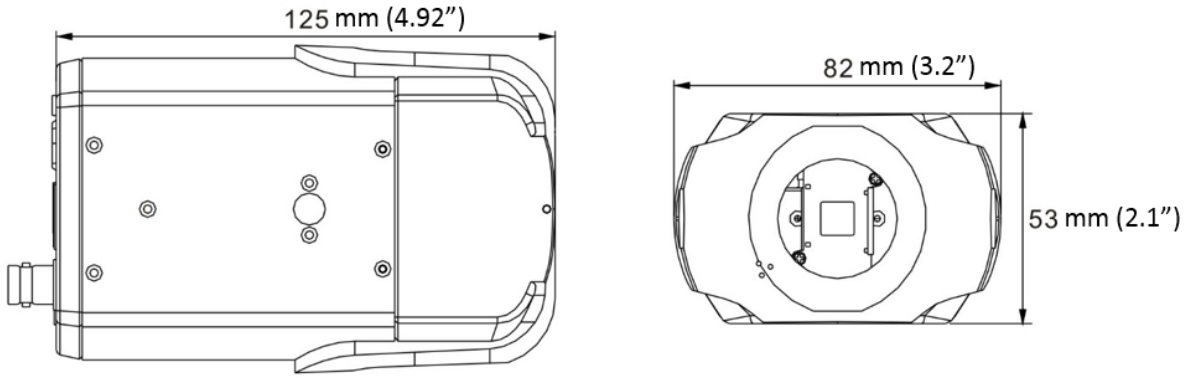


Figure 2: CF-5212/CF-5222 Camera Dimensions

3.2 Camera Connections

Figure 3 shows the various connectors and reset button contained within the housing of the CF-5212 and CF-5222 cameras. The connectors, pin numbers and signal definitions related to each pin are listed in Table 1.

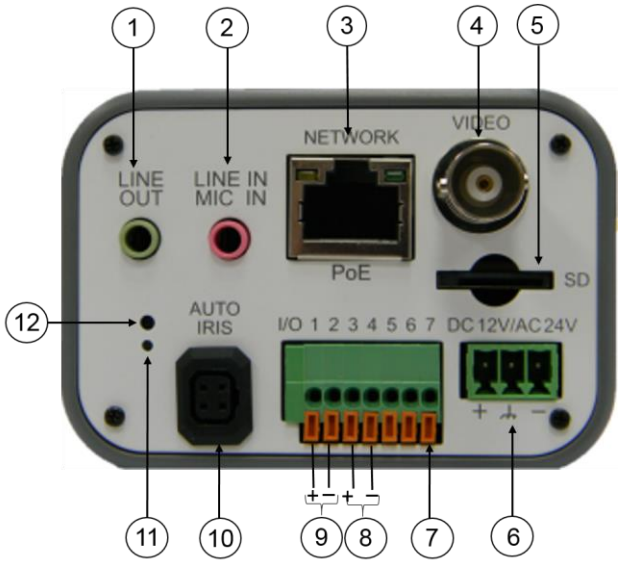


Figure 3: CF-5212/CF-5222 Camera Input/Output Connections

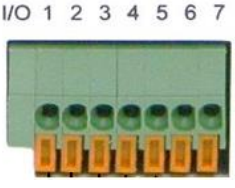
Table 1: CF-5212/CF-5222 Camera Connector Panel Description

ID	Connector Name	Pin No./ Connector Type	Definition	Description
1	**Line Out**		Audio out	2-way audio transmission
2	**Line In/Mic In**		Audio in	
3	**PoE Network**	RJ45, Network LEDs	10/100 Mbps Ethernet/PoE	Power over Ethernet
4	**Video**	BNC	Analog video	For video output
5	**SD**		microSD card slot	Not supported
6	**DC 12V/AC 24V**	1 – Power (+) 2 – Reserved 3 – GND (-)	12V DC	Power supply connection indication (green LED)
		1- Power (+) 2- Earth GND 3- Power (-)	24V AC	
7 to 9	**I/O 1 to 7**	1 - Output (+) 2 - Output (-)	Alarm output	7-terminal connection block
		3 - Input (+) 4 - Input (-)	Alarm input	
		5 – GND	Grounding	
		6 - D (-) 7 - D (+)	Reserved Do NOT connect	
10	**Auto Iris**	DC iris lens connector	DC iris port	
11	**PWR**	N/A	Power LED	Power indication
12	**RESET**	N/A	Reset	Recycles the unit

3.2.1 Alarm Input/Output Pin-out

The alarm input and output connections are shown below.

Table 2: Input/Output Alarm Connections

Pin No.	Designation	Terminal Block Alarm Connections
1	Output (+)	
2	Output (-)	
3	Input (+)	
4	Input (-)	

4 System Requirements

To access the CF-5212/CF-5222 fixed IP camera via a web browser, ensure that your PC has the proper network connection and meets the system requirements described below.

Table 3: System Requirements

Item	Camera Client Application System Requirements
Personal Computer	Intel® Pentium® M, 2.16 GHz or Intel® Core™2 Duo, 2.0 GHz 2GB RAM or better
Operating System	Windows 7, 8, or 8.1
Web Browser	Microsoft Internet Explorer 9, 10, 11
Network Card	10Base-T (10 Mbps) or 100Base-TX (100 Mbps) operation
Viewer	ActiveX control plug-in for Microsoft IE

5 Installation

Follow the instructions below for indoor installation of the ioimage HD CF-5212/CF-5222 series camera.

5.1 Indoor Installation

Read the instructions provided in this chapter thoroughly before installing the CF-5212/CF-5222 camera. The following points are additional considerations for indoor installation:

- There must be a fuse or circuit breaker at the starting point of the electrical wiring infrastructure.
- For indoor installations, such as industrial applications, the CF-5212/CF-5222 camera must be protected from hostile external elements (e.g. corrosive environment, metallic dust, extreme temperatures, soot, moisture, over spray, etc.)
- Do not place the CF-5212/CF-5222 camera on or near radiators and heat sources.
- All electrical work must be performed in accordance with local regulatory requirements.

Related Links

- Power and Ethernet Cable Connection
- Initial Camera Configuration
- Mounting Instructions
- Adjusting and Framing-Up the Camera View

5.2 Power and Ethernet Cable Connection

Power Connection

Make sure the camera's power cable is properly connected. Refer to Table 1: CF-5212/CF-5222 Camera Connector Panel Description. If using Power over Ethernet (PoE), make sure Power Sourcing Equipment (PSE) is available on the connected network. All electrical work must be performed in accordance with local regulatory requirements.

Ethernet Cable Connection

A Cat 5 Ethernet cable is recommended for network connection. For best transmission quality, the cable length should not exceed 100 meters (328 feet). Connect one end of the Ethernet cable to the CF-5212/CF-5222 camera and the other end of the cable to the network switch or PC.

Note:
An Ethernet crossover cable can be used when connecting the CF-5212/CF-5222 camera directly to the PC.

Check the status of the link indicator and activity indicator LEDs. If the LEDs are unlit, check the LAN connection.

Table 4: Network Port LED Indications

RJ45 Connector	LED	Description
	**Green**	Link Light - indicates a stable network connection
	Yellow	Activity Light - flashes to indicate network activity

5.3 Lens Mounting

Before installing your camera, install the camera lens.

Note:

The camera lens is sold separately and should be selected to match the needs of the scene and to optimize the use of the camera capabilities. See Mounting and Lens Accessories.

5.3.1 Selecting the Proper Lens

5.3.1.1 DC Auto Iris vs. Manual Iris Lens

A DC auto iris lens is required when operating the camera in *Auto Iris* exposure mode. *Auto iris* mode is recommended for use in indoor environments with mixed lighting sources, where the main source is fluorescent lighting and natural lighting enters the scene through windows and other exposed areas. In all other cases, *Auto Shutter* exposure mode is recommended. The camera can operate in one of the following three exposure modes: *Manual* (using set values for shutter and iris), *Auto Iris,* and *Auto Shutter*. *Auto Shutter* and *Manual* modes do not require an auto iris lens. A manual iris lens can be used instead.

5.3.1.2 Focal Length

Focal length determines the scene's viewing angle, or, in other words, the dimensions of the scene which will be generated by the camera. The trade-off for focal length is between the width of the scene and the magnification of objects appearing in the scene. The longer the focal length is, a narrower scene will be achieved, while the size of objects will increase. Greater size means that more pixels will be used to represent each object, and greater level of details will be present.

In a similar manner, the shorter the focal length is, the smaller the size of each object will be, while the captured scene will become wider.

Note:

Use a short focal length to cover a wide area and detect objects at close distances. Use a long focal length to achieve greater detection distances while narrowing the field of view.

After you select your lenses and see the amount of detail provided, consider your security surveillance coverage, camera locations, and any additional needs that may be discovered. Consult your DVTEL representative if you have any questions.

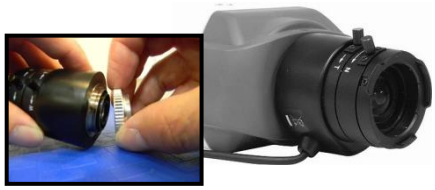
To mount a lens on the CF-5212/CF-5222 camera

1. Remove the plastic insert covering the threaded camera lens mount.

> **Tip:**
> Do not touch the sensor or allow dust to accumulate in the lens mount.

2. If you are using a C-mount lens, screw a 5mm adapter ring into the C-mount to convert it to a CS-mount (see figures below).

C to CS-Mount Adapter



Completion

> **Note:**
> A C- to CS adapter is NOT included with the camera.

3. Align the lens threads into the lens mount and screw on the lens.
4. If your lens has a DC auto iris, plug the auto iris cable from the motorized lens assembly into the AUTO IRIS port of the camera.

Figure 4: Auto Iris Port Connection

> **Tip:**
> If there are problems focusing, it might be necessary to make a back focus adjustment. See Back Focus Adjustment (page 97).

5.4 Initial Camera Configuration

To perform the initial camera configuration

1. Unpack the camera and remove the protective cover.
2. Remove the PE cloth sheet and lens cap.
3. Connect one end of the Cat 5 Ethernet cable to the Ethernet port of the camera and the RJ45 connector at other end to the Power Sourcing Equipment (PSE) device, such as a switch.
4. Verify that the RJ45 connector LEDs illuminate green (indicating a stable network connection) and flashing yellow (to indicate network activity).
5. Copy and run the `dna.exe` file from the included CD.

> **Note:**
> DNA is an enhanced software alternative to Device Search. Both are supplied on the included CD. Either of these programs may be used. ioimage HD is supported by DNA version 2.0.4.1 and above.

   a. Mark the unit requiring IP assignment.

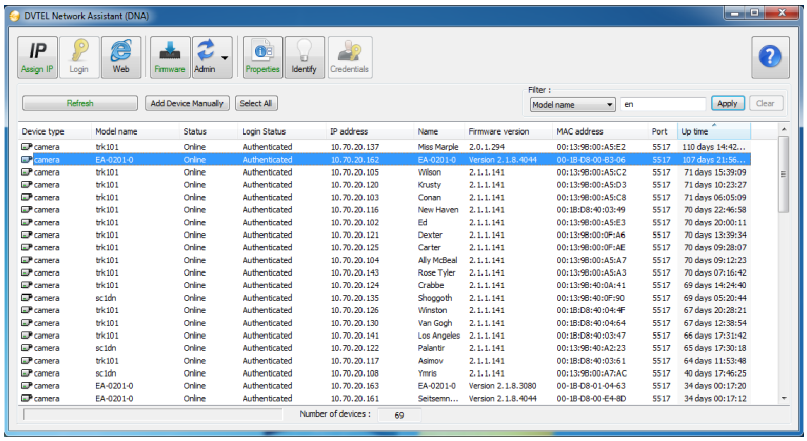


Figure 5: Discovered IP Devices

   b. Right-click on the mouse and select the assigned IP or press the **Assign IP** button to open the DNA **Assign IP** screen.

   c. In the dialog box that is displayed, enter values for the IP Address, Gateway and Netmask.

d. Click **Update** and wait for ✔ *OK* status to be displayed.

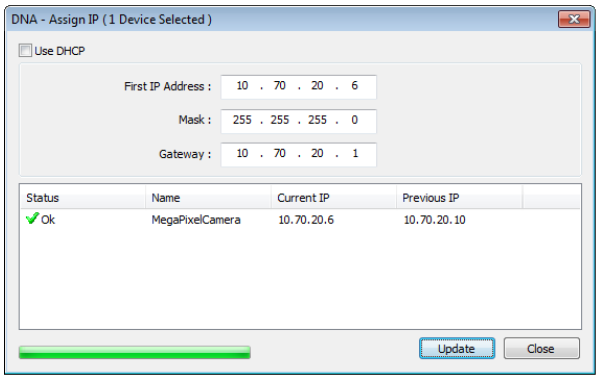


Figure 6: Assign IP Dialog Box

6. Disconnect the Ethernet cable. The camera is ready for deployment (mounting) in a site installation.

Note:

The camera can be connected to a PC for bench installation via an Ethernet cross-cable.

Note:

The camera default IP Address and the subnet mask IP Address are automatically supplied by the DHCP server.

Tip:

A camera setup adapter, such as Veracity Pinpoint, can be used to connect a laptop directly to the camera when using PoE.

5.5 Mounting Instructions

The following are mounting instructions for the CF-5212 and CF-5222 fixed IP cameras.

Caution:

To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit's requirements (cooling/heating). Operating temperature should be kept in the range specified for the product (0° to 50°C/32° to 122°F, with no more than 90% relative humidity, non-condensing).

Attention:

Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la régulation de température est suffisante pour répondre aux exigences de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage de température spécifiée pour le produit (0° à 50°C/32° à 122°F), sans condensation d'humidité supérieur à 90%.

To mount the camera, follow one of these procedures:

- For indoor installations without a housing:
  a. On the ceiling/wall/flat surface, install a security camera wall mount bracket stand that is sturdy enough to hold the camera in a fixed position for the field of view required.
  b. Screw the bracket/stand to the mounting socket on the bottom of the camera.
  c. Connect the cables and wiring to the camera. See Figure 3: CF-5212/CF-5222 Camera Input/Output Connections and Table 1.
- For indoor/outdoor installations using a typical protective camera housing:
  a. Thread the wires through any of the infrastructure and brackets (e.g. pole bracket/corner bracket/etc.) as needed as well as through the wall bracket arm.
  b. Bolt the wall bracket (arm) to the prepared surface.
  c. Loosen the screws or unlatch the camera housing lid, open the housing and loosen the plastic cable glands (cable fittings).
  d. Thread the cables through the cable glands into the camera housing.

Figure 7: Cable Gland

  e. Attach the camera housing to the wall bracket (arm) using the provided screws and wrench.
  f. Remove the housing plate (base for camera) and using the provided camera mount screw, thread the screw through the plate into the camera's bottom mounting socket.
  g. Put the camera mounted on the base plate back in the housing. Adjust forward positioning when you adjust the lens.
  h. For housings with internal blowers and heaters, connect the wiring to the camera housing terminals (power input) according to the manufacturer's instructions for heaters (heater output) and fans (blower output) that the camera housing features. Connect any ground (GND) to the camera housing ground connection.
  i. Connect the cables and wiring to the camera. See Figure 3: CF-5212/CF-5222 Camera Input/Output Connections.

> **Note:**
>
> For outdoor installation, the camera must be installed in a protective housing such as a DVTEL CF-X200-00 camera housing. See the figure below.

Figure 8: DVTEL CF-X200-01 Camera Housing with Bracket

6 Using the DNA Utility to Search and Access the Camera

The DVTEL Network Assistant (DNA) is a user-friendly utility that is designed to easily discover and configure DVTEL edge devices on a network. The DNA tool has a simple user interface and does not require any installation. The software is provided as a single, standalone executable. It runs on any PC.

DNA provides a central location for listing all the DVTEL camera models accessible over the network. Once listed, each camera can be right-clicked to access and change the network settings. If the network settings are changed for some reason, a new search will relist the units. The units may then be configured via the web interface.

If DVTEL Latitude is being used, configure the unit with a static IP address rather than with DHCP. This ensures that the IP address will not automatically change in the future and interfere with configurations and communication. The camera must be made accessible for the network's addressing.

Note:

ioimage HD is supported by DNA version 2.0.4.1 and above. For detailed guidelines about DNA and its usage, refer to the *DNA 2.0 User Manual*, which is included in the CD provided with the camera. You can also download the manual from the *Downloads* tab at http://www.dvtel.com/products-solutions/tools/.

7 Using the Web Browser to Access the Camera

Use the DVTEL Camera Viewer (DCViewer) web player software to access the camera, configure its properties, and view video through your web browser.

Note:

Users who have previously installed the DCViewer application on the PC should delete the existing DCViewer from the PC before accessing the camera. For information on how to uninstall and clear Temporary Internet Files, see Deleting the Existing DCViewer (page 95).

To install the DCViewer software online

1. Open your web browser and type the camera's IP address which appears in the DNA address bar. Upon initial connection to the camera, a prompt to install the DCViewer application appears. Click **Allow**.
2. Do one of the following:
   - If the web browser does not allow DVTEL Web Player to install, check the Internet security settings or ActiveX controls and plug-in settings to continue the process. See Internet Security Settings.
   - If the following screen is displayed, click the link to install the ActiveX component.

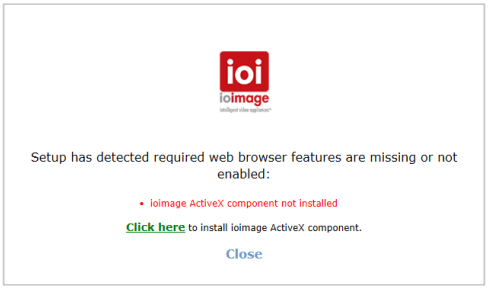


Figure 9: ActiveX Installation Message

A dialog box opens, requesting you to install the `render.cab` file. Click **Install**. The application closes and reopens on the **Home** page.

- If the Information Bar (just below the URL bar) prompts for permission to install the ActiveX Control for displaying video in the browser (see the figure below), right-click on the Information Bar. Select **Install ActiveX Control** to allow the installation.

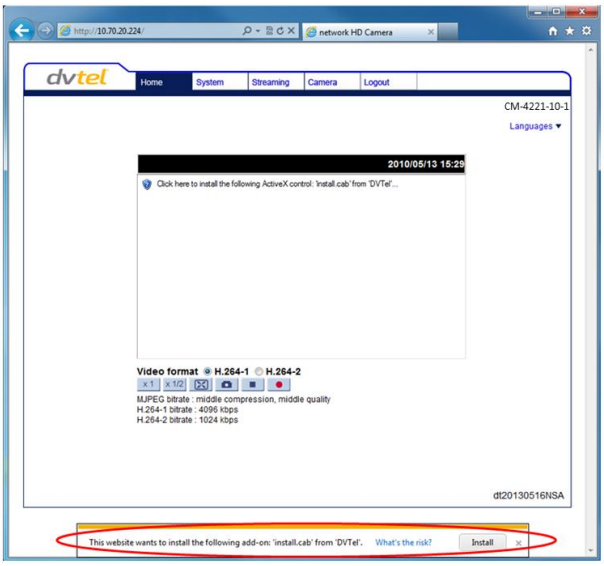


Figure 10: Installing the ActiveX Control

- If a security warning window prompt appears, click **Install**.

Figure 11: Security Window

3. Follow the instructions to complete installation of the DCViewer application in the wizard.

Note:

If the password is changed and DVTEL Latitude AdminCenter Discovery feature is in use, deselect all other proprietary types. Select *DVTEL HD Series* so that the new password can be configured in the Latitiude Discovery tab settings.

8 Adjusting and Framing-Up the Camera View

After the camera is connected to the network and is running, it is necessary to frame-up the scene and adjust the camera settings to optimize the picture for the individual scenes. If Latitude is being used, consider scheduling different settings for changing ambient conditions throughout the day, week, month or seasons.

To adjust and frame-up the camera view

1. In the DNA application, click **DNA**.
2. In the Discovery list, click to select the camera.
3. Right-click the context menu and select **Browse**, or enter the camera's IP address in your browser's URL address bar.
4. When the browser connects to the camera and prompts for login, do the following:
   a. Log in using the default user name *admin* and password *admin*. Note that both are case sensitive. If the password has previously been changed, use the new password.
   b. Allow the ActiveX to download and choose to install the DVTEL Web Player (DCViewer).

> **Tip:**
> To view greater image detail for more accurate high-definition focusing, on the web interface **Home** page, click the **Full Screen** button and use the full screen view to check the focus.

> **Note:**
> Best focusing results can be achieved when the lens iris is fully open (such as at night in low light). This prevents loss of sharpness if light levels are reduced at night.

To achieve this during the day, in the web interface, go to the **Camera > Exposure** screen and select *Auto Shutter* mode. Save changes and complete the focusing steps. When finished, restore your exposure settings as needed.

5. Adjust the pan and tilt as follows:

- For indoor installations without a housing:

   a. Loosen the tension screw on the bracket/stand and move (pan and tilt) the camera so that the field of view is optimized for your scene and retighten the tension bolt to hold the camera in place.

   b. On the camera, adjust the zoom ring and focus ring on the camera lens for your scene. If you have a manual iris, also adjust the iris ring on your lens.

Figure 12: Camera Lens Zoom and Focus Adjustment

- For indoor or outdoor installations using a protective camera housing

a. Support the camera housing and loosen sufficiently the tension bolt on the bracket Pan/Tilt assembly so that it allows you to reposition the camera housing.

Figure 13: Camera Housing Repositioning

b. Move the housing so that the camera field of view is optimized for your scene and retighten the tension bolt on the wall bracket Pan/Tilt assembly.

c. On the camera, adjust the zoom ring and focus ring on the lens for your scene. If you have a manual Iris, also adjust the iris ring on your lens. See Figure 12.

d. Adjust the camera and base plate by moving it either forward or backward so that the camera lens close enough to the glass that it reduces the possibility of reflection but does not make contact with the glass.

e. Tighten the base plate securely in place and close the camera housing lid.

f. Close the latch or tighten the screws firmly so that the lid seal is properly maintained.

9 Configuration and Operation

The ioimage HD camera is provided with a browser-based configuration interface for video playback and recording. If DVTEL's Latitude VMS is used, many of the configurations and features of DVTEL's VMS provide additional configuration and automation options for the camera.

This section includes the following information:

9.1 Browser-Based Viewer Introduction

The figure below shows the ioimage HD camera's browser-based user interface.

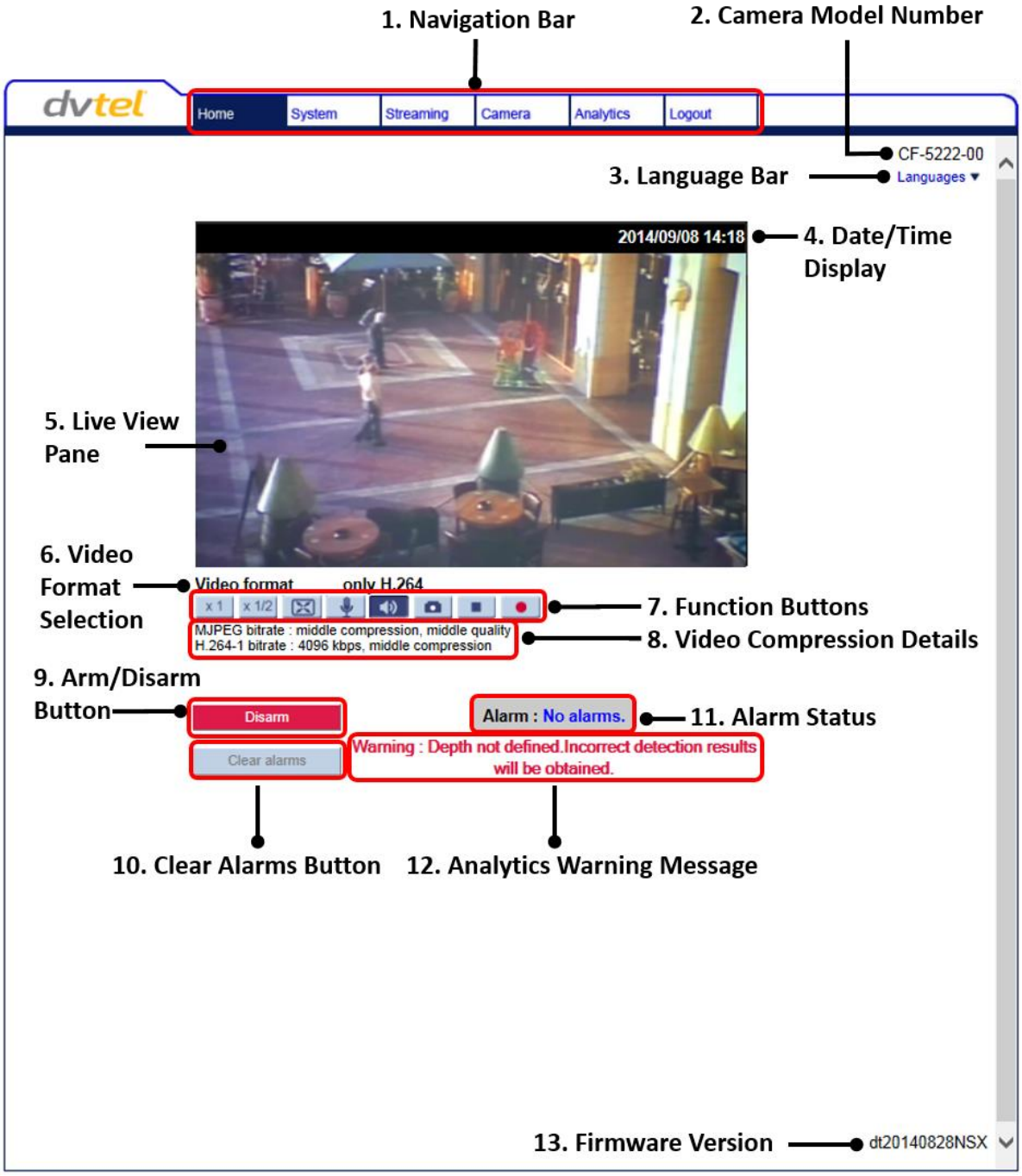


Figure 14: ioimage HD Browser-Based User Interface

The following items are displayed on the screen:

1. At the top of the Viewer window is the Navigation Bar, which contains six tabs: **Home, System, Streaming, Camera**, **Analytics,** and **Logout.**

    - Home
      Users can monitor live video of the targeted area, adjust the display size including use of the digital zoom feature, activate or de-activate the speaker (audio function), take snapshots of the view area, stop/start video streaming, and record video in a designated storage place. Further details are discussed in Home Page.
    - System
      The administrator can set host name, system time, root password, network related settings, etc. Further details are discussed in System-Related Settings.
    - Streaming
      The administrator can modify video resolution and picture rotation and select audio compression mode from this tab. Further details are discussed in Video and Audio Streaming Settings.
    - Camera
      The administrator can adjust many camera settings from this tab, such as Exposure, White Balance, Picture, Backlight, Digital Zoom, IR Function, WDR Function, Noise Reduction, and TV System. Further details are discussed in Camera-Related Settings.
    - Analytics
      The administrator can configure analytic settings from this tab. Further details are discussed in Analytics.
    - Logout
      Click the tab to re-login the camera with another username and password. See Logout.

2. The camera model number is displayed in the top right-hand corner of the screen.
3. The Language Bar is located under the camera model number. Supported languages include English, German, Spanish, French, Italian, Japanese, Korean, Portuguese, Russian, Simplified Chinese, and Traditional Chinese.
4. The date and time are displayed under the Language Bar.
5. In the center of the Viewer window is the *Live View* pane, which displays the image that the camera is monitoring.
6. The selected video format is displayed under the *Live View* pane.
7. Below the video format selection are the Function buttons, which are discussed in the following section.
8. Under the Function buttons are the video compression details, including bit rate, compression, and quality.
9. The **Arm/Disarm** button is displayed under the Function buttons.
10. The **Clear Alarms** button is displayed under the **Arm/Disarm** button.
11. The alarm status is displayed to the right of the **Arm/Disarm** button.
12. The Analytics Warning message is displayed under the Alarm Status, indicating if analytics have not been configured properly.
13. The firmware version of the camera is displayed in the bottom right-hand corner of the screen.

9.2 Home Page

The CF-5212/CF-5222 camera includes the following function buttons located on the **Home** page, as shown below.

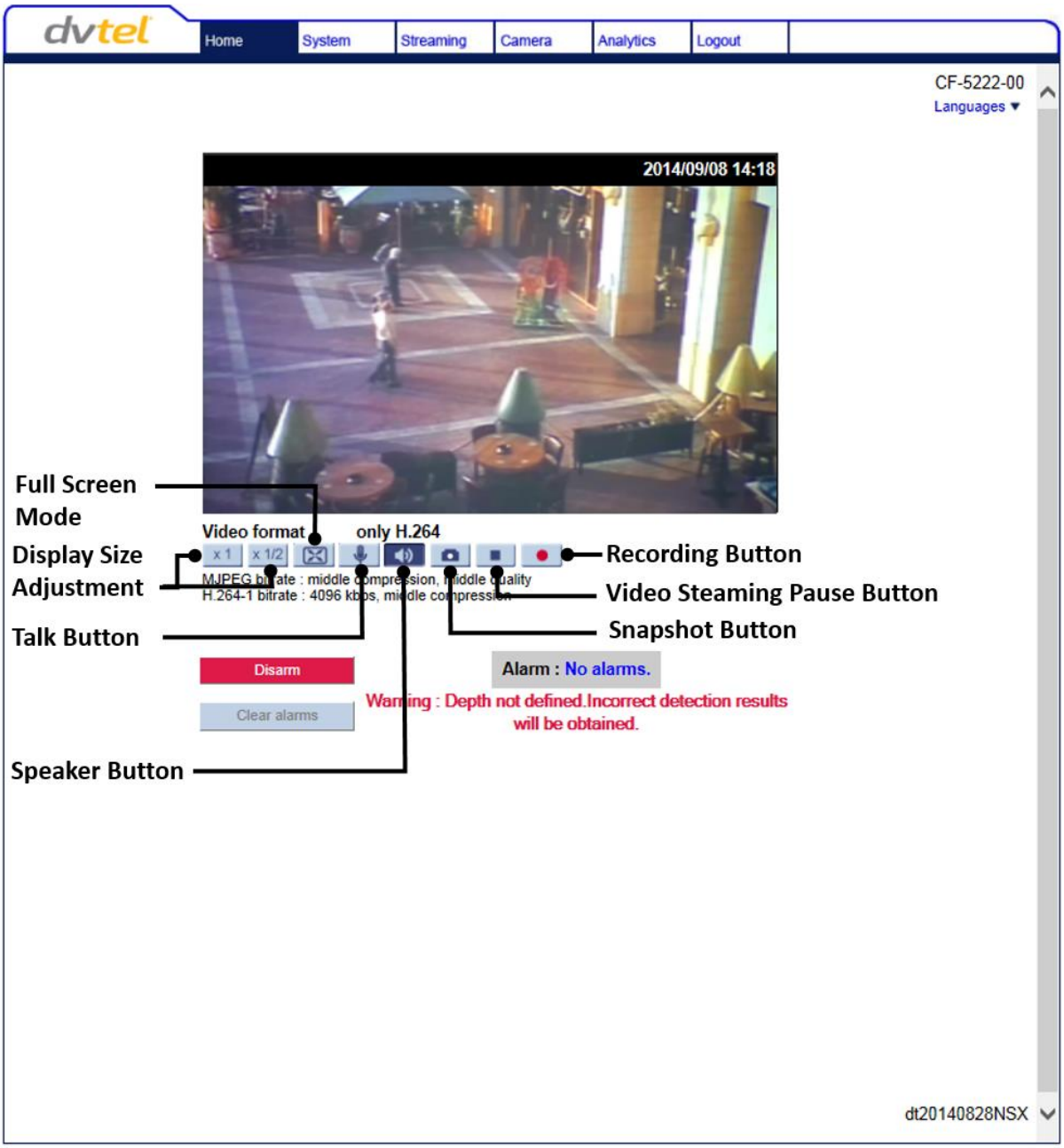


Figure 15: Home Page Function Buttons

- **Display Size Adjustment (x1/x½)**
  The image display size can be adjusted to full-size or half-size.
- **Full Screen Mode** (with Digital Zoom Control)
  Click this button to view the monitored image in full screen mode. Use the mouse to control zoom effects in Full Screen mode: scroll the mouse wheel (for zoom in/out), and drag the mouse into any direction. Double-click on the screen to exit Full Screen mode and return to the **Home** page.

- **Talk**
  The **Talk** button allows the local site to talk to the remote site. Click the button to switch it on/off. This function is available only to a user who has been granted this privilege by the Administrator. Refer to User in the Security section for further details.
- **Speaker**
  Press the **Speaker** button to mute/activate the audio. This function is available only to a user who has been granted this privilege by the Administrator. Refer to User in the Security section for further details.
- **Snapshot**
  Press this button to automatically save the JPEG snapshots in the specified location. The default location to save snapshots is: C:\.To change the storage location, refer to File Location.
- **Video Streaming Stop/Restart**
  Press the **Stop** button to disable video streaming and to display the live video as black. Press **Restart** to show the live video again.
- **Recording**
  Pressing the **Recording** button stores recordings from the Live View in the location specified on the local hard drive, which can be configured in the **File Location** screen. The default storage location for the web recording is: C:/. Refer to File Location for details.

9.3 System-Related Settings

The figure below shows all categories under the **System** tab. Each category in the sidebar is explained in the following sections.

Note:
The **System** configuration screen is accessible only by the Administrator.

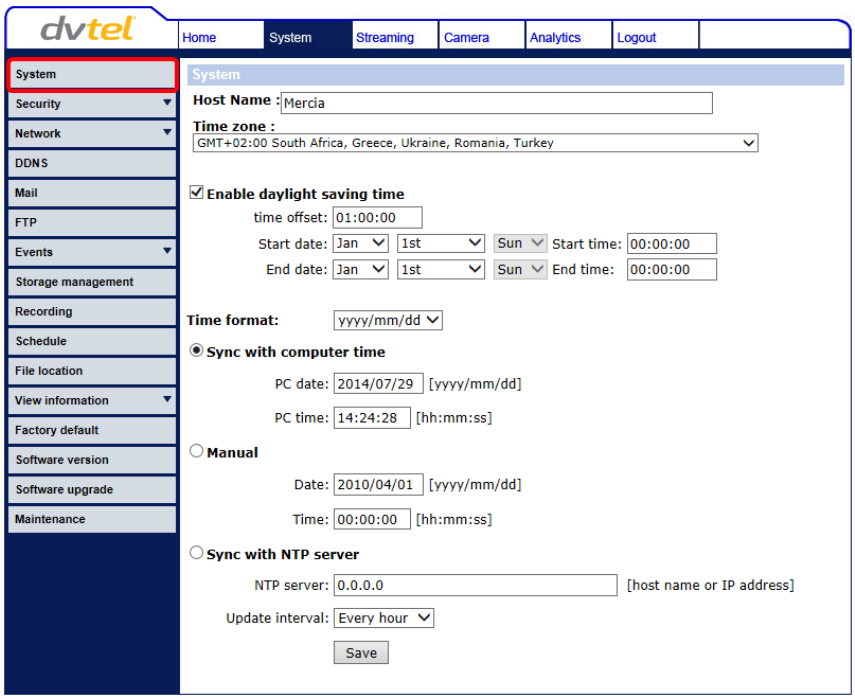


Figure 16: System Screen

Related Links

- System
- Security
- Network
- DDNS
- Mail
- FTP
- Events
- Storage Management
- Recording
- Schedule
- File Location
- View Information
- Factory Default
- Software Version
- Software Upgrade
- Maintenance

9.3.1 System

Click the **System** tab in the sidebar. The **System** screen is displayed in Figure 16: System Screen. It includes the following details:

Host Name

The host name is for camera identification. If the alarm function is enabled and is set to send an alarm message by Mail/FTP, the host name entered here is displayed in the alarm message. See Events > Application.

Time Zone

Select the time zone from the drop-down list.

Enable Daylight Saving Time

To enable daylight savings time, select the checkbox, specify the time offset, and enter the start date and end dates for daylight savings time. The format for time offset is [hh:mm:ss]. For example, if the amount of time offset is one hour, enter 01:00:00 in the field.

Time format

Enables a choice of formats: either year, month and day (yyyy/mm/dd) or day, month and year (dd/mm/yyyy).

Sync with Computer Time

Select this button to synchronize video date and time display with the PC.

Manual

Select this button to set video date, time and day manually. Entry format should be identical with that shown next to the **Enter** field.

Sync with NTP Server

Network Time Protocol (NTP) is an alternate way to synchronize the camera's clock with an NTP server. Specify the server to synchronize in the **Enter** field. Then select an update interval from the drop-down list. For further information about NTP, visit www.ntp.org.

9.3.2 Security

Clicking the **Security** tab in the **System** screen opens a drop-down list with the tabs **User**, **IP Filter,** and **IEEE 802.1X**.

Related Links

- User
- IP Filter
- IEEE 802.1X

9.3.2.1 User

Click the **User** tab in the **Security** category on the sidebar to display user credentials.

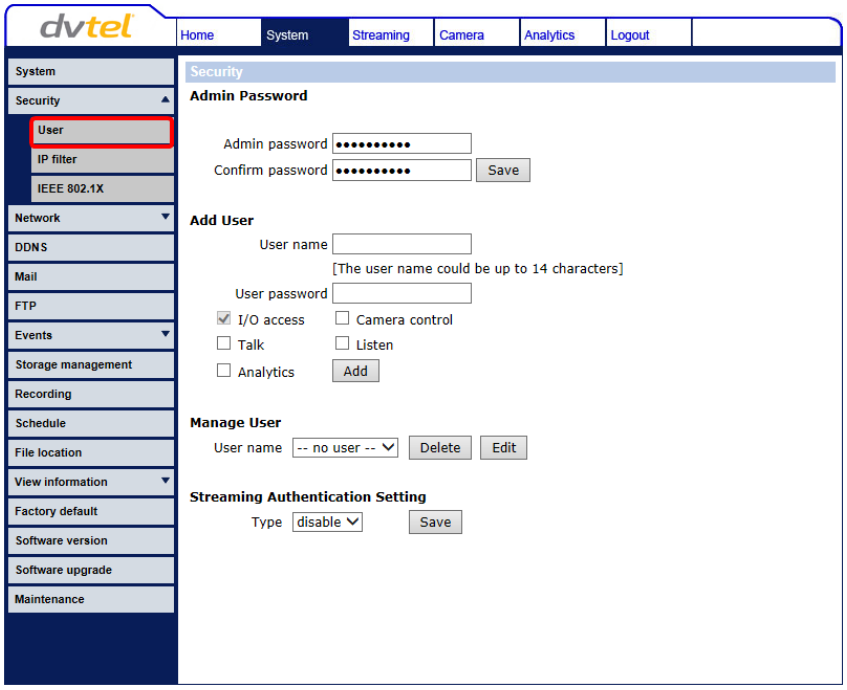


Figure 17: Security > User Screen

Admin Password

Change the administrator's password by entering the new password in both text boxes. The input characters/numbers are displayed as dots for security purposes. After clicking **Save**, the web browser asks the Administrator for the new password (maximum 14 digits).

Note:
The following characters are valid: A-Z, a-z, 0-9,!#$%&'-.@^_~.

Add user

The user name and passwords are limited to 14 characters. There is a maximum of 20 user accounts.

To add a new user

1. Type the new user name and password in the respective fields**.**
2. Select the appropriate check boxes to give the user I/O Access, Camera Control, Talk, Listen, or Analytics permissions.
   - *I/O access* – Basic functions that enable the user to view video when accessing the camera.
   - *Camera control* – Allows the user to change camera parameters on the **Camera** tab.
   - *Talk* – Allows the user at the local site to talk to the administrator at the remote site.
   - *Listen* – Allows the user at the local site to listen to the administrator at the remote site.
   - *Analytics* – Allows the user to define analytic parameters from the **Analytics** tab.
3. Click **Add**.

Manage User

- To delete a user, pull down the user list and select the user name to delete. Click **Delete** to remove it.
- To edit a user, pull the user list down and select a user name. Click **Edit** to edit the user's password and privileges.

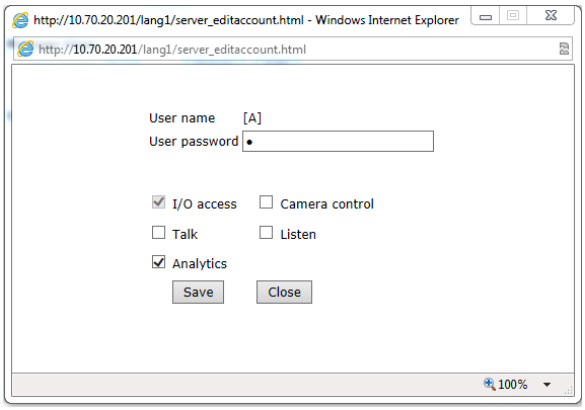


Figure 18: Editing Password and Privileges

Note:

You must enter the user password and also select the authorized function(s). When finished, click **Save** to modify the account authority.

Streaming Authentication Setting

From the drop-down list, select one of the following options:

- *Disable* – Do not use streaming authentication (default setting).
- *Basic* – A form of authentication that uses unencrypted base64 encoding. Basic Authentication should generally only be used where transport layer security, such as HTTPS, is provided.
- *Digest* – A form of authentication used over RTSP in which credentials are encrypted when transmitted.

9.3.2.2 IP Filter

The IP filter restricts access to the camera by denying/allowing specific IP addresses. Click the **IP filter** tab under **Security** in the sidebar to display the following screen.

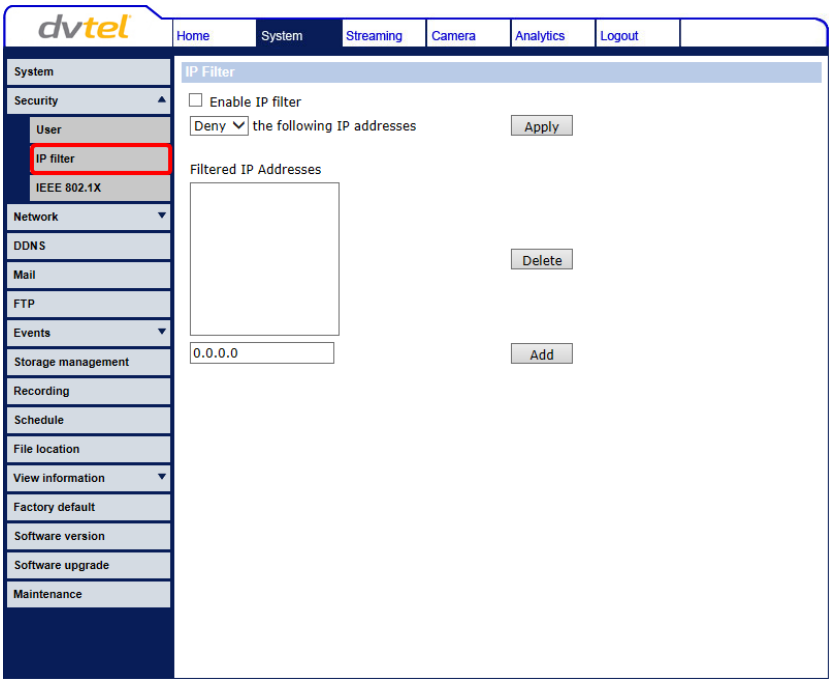


Figure 19: IP Filter Screen

To enable the IP filter

1. Check the box to enable the *IP Fil*ter function. Once enabled, the listed IP addresses (IPv4) are allowed/denied access to the camera.
2. Select **Allow** or **Deny** from the drop-down list.
3. Click the **Apply** button to determine the *IP Filter* behavior.

To add or delete an IP address

1. Enter the IP address in the *Filtered IP Addresses* text box.
2. Click **Add** to add a new filtered address. The *Filtered IP Addresses* box shows the currently configured IP addresses. Up to 256 IP address entries may be specified.
3. To remove an IP address from the list, select the IP address and then click **Delete**.

9.3.2.3 IEEE 802.1X

The camera is allowed to access a network protected by 802.1X/EAPOL (Extensible Authentication Protocol over LAN). Users must contact the network administrator to obtain certificates, user IDs, and passwords.

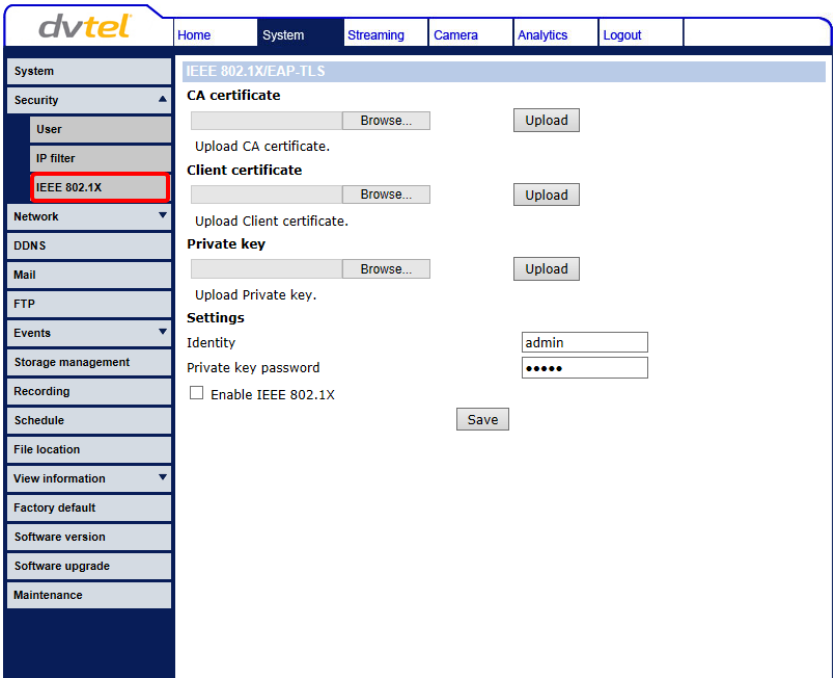


Figure 20: IEEE 802.1X/EAP-TLS Screen

CA Certificate

The CA certificate is created by the Certificate Authority for the purpose of validating itself. Upload the certificate to check the server's identity.

Client Certificate/Private Key

Upload the Client Certificate and Private Key to authenticate the camera.

Settings

- *Identity* – Enter the user identity associated with the certificate. Up to 16 characters can be used.
- *Private Key Password* – Enter the password associated with the user identity. Up to 16 characters can be used.

Enable IEEE 802.1X

Check the box to enable *IEEE 802.1X.* The setting is disabled by default. Click **Save** to save the IEEE 802.1X/EAPTLS setting.

9.3.3 Network

From the **System** screen, click the **Network** tab. A drop-down list appears with tabs including **Basic**, **QoS**, **SNMP**, and **UPnP**.

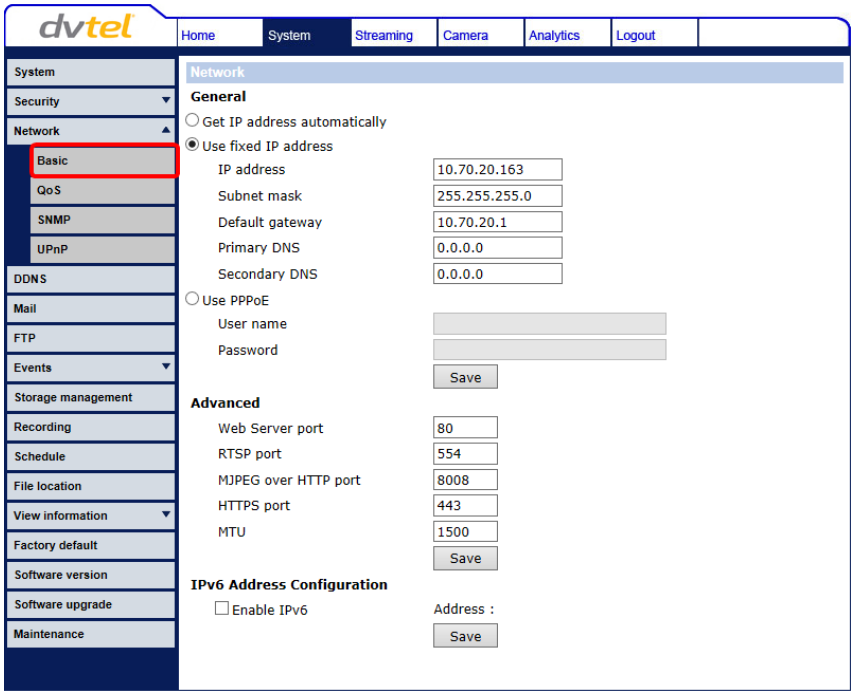


Figure 21: Network Screen

Related Links

- Basic
- QoS (Quality of Service)
- SNMP Settings
- UPnP

9.3.3.1 Basic

You can connect to the camera with either fixed or dynamic (DHCP) IP address. The camera also provides PPPoE (Point-to-Point Protocol over Ethernet) support for users who connect to the network via PPPoE.

The screen is divided into three sections: General, Advanced and IPv6 Configuration. See Figure 21: Network Screen.

14. General

Select one of the following options in the *General* area for configuring network settings:

- **Get IP address automatically (DHCP)**

If you select *Get IP address automatically*, you can use the DNA utility, which is provided in the supplied CD, to obtain the IP address. See Using the DNA Utility to Search and Access the Camera.

Note:

For future reference, record the camera's MAC address, which is found on the camera label.

- **Use fixed IP address**

The camera's default setting is *Use fixed IP address*. You may use DNA or enter the IP address in your browser's URL address bar.

To set up a new static IP address

1. Select the Use fixed IP address option.
2. Enter the following information:
   - *IP address* – The IP address is necessary for network identification.
   - *Subnet mask* – Used to determine if the destination is in the same subnet. The default value is 255.255.255.0.
   - *Default gateway* – Used to forward frames to destinations in a different subnet. An invalid gateway setting causes transmission to destinations in other subnets to fail.
   - *Primary DNS* – The primary domain name server that translates host names into IP addresses.
   - *Secondary DNS* – A secondary domain name server that backs up the primary DNS.
   - *Use PPPoE* – PPPoE users should enter their PPPoE user name and password into the respective fields.
3. Click **Save** to confirm the settings.

15. Advanced

Enter the following advanced parameters in the *Advanced* section of the screen:

- *Web Server port* – The default web server port is *80*. Once the port is changed, the user must be notified the change for the connection to be successful. For instance, when the Administrator changes the HTTP port of the camera whose IP address is 192.168.0.100 from 80 to 8080, the user must type in the web browser http://192.168.0.100:8080 instead of http://192.168.0.100.

  Note:
  If you change the default HTTP port number and are using Latitude, you must rediscover the unit.

- *RTSP port* – The default setting of the RTSP port is *554.* The range is from *1024* to *65535*.
- *MJPEG over HTTP port* – The default setting of MJPEG over HTTP port is *8008*. The range is from *1024* to *65535*.
- *HTTPS port* – The default setting of HTTPS port is *443*. The range is from *1024* to *65535*.
- *MTU* – The MTU (Maximum Transmission Unit) is the greatest amount of data that can be transferred in one physical frame on the network. For Ethernet, the MTU is *1500* bytes (default setting). For PPPoE, the MTU is *1492*. The range is from *700* to *1500* bytes.

  Note:
  Be sure to assign a different port number for each separate service mentioned above.

Click **Save** to save the settings.

16. IPv6 Address Configuration

IPv6 is not supported in this version.

9.3.3.2 QoS (Quality of Service)

QoS provides differentiated service levels for different types of traffic packets and guarantees delivery of priority services during periods of network congestion. Adapting the Differentiated Services (DiffServ) model, traffic flows are classified and marked with DSCP (DiffServ Code point) values, and as a result receive the corresponding forwarding treatment from DiffServ-capable routers.

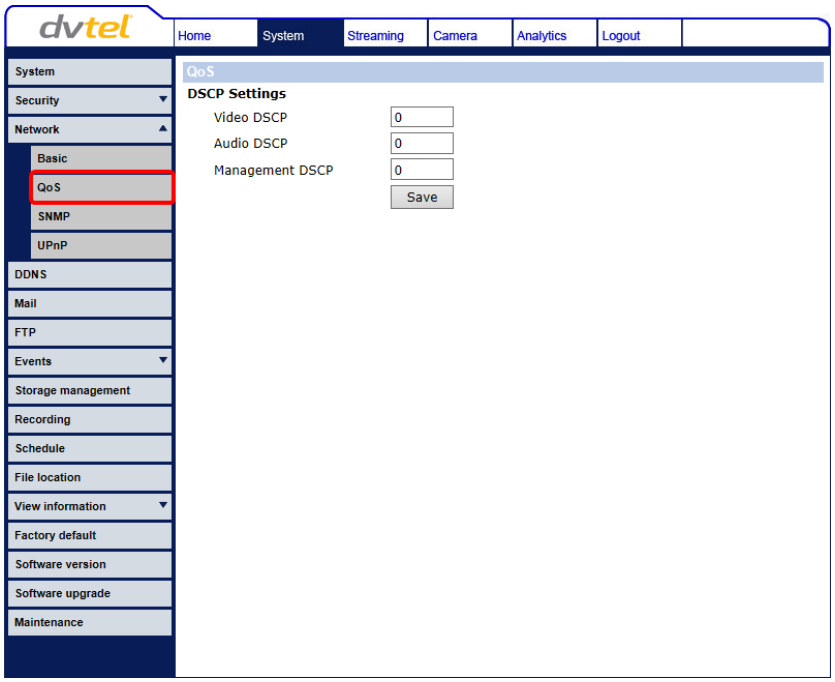


Figure 22: QoS Screen

DSCP Settings

The DSCP value range is from 0 to 63. The default DSCP value is 0 (DSCP disabled). The camera uses the following QoS classes: Video, Audio, and Management.

- *Video DSCP* – This class consists of applications such as MJPEG over HTTP, RTP/RTSP and RTSP/HTTP.
- *Audio DSCP* – The cameras support audio.
- *Management DSCP* – This class consists of HTTP traffic (web browsing).

Click **Save** when complete.

Note:

To enable this function, make sure the switches/routers in the network support QoS.

9.3.3.3 SNMP Settings

Simple Network Management Protocol (SNMP) enables the camera to be monitored and managed remotely by the network management system.

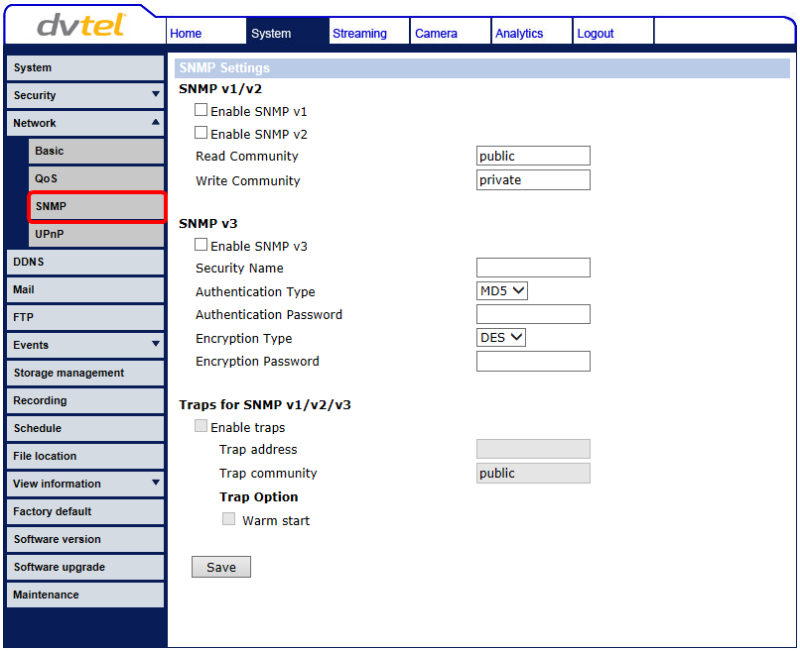


Figure 23: SNMP Settings Screen

SNMP v1/v2

- *Enable SNMP v1* or *Enable SNMP v2* – Select the version of SNMP (v1 or v2) to use by checking the relevant box.
- *Read Community* – Specify the community name that has read-only access to all supported SNMP objects. The default value is *public.*
- *Write Community* – Specify the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is *private.*

SNMP v3

SNMPv3 provides important security features including:

- Confidentiality – Encryption of packets to prevent snooping by an unauthorized source.
- Integrity – Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism.
- Authentication – To verify that the message is from a valid source.

To enable the SNMP v3 protocol, enter the appropriate data and passwords requested:

- *Enable SNMP v3* – Select the checkbox.
- *Security Name* – See note below.
- *Authentication Type* – Select MD5 or SHA from the drop-down list. See note below.
- *Authentication Password* – See note below.
- *Encryption Type* – Select DES or AES from the drop-down list. See note below.
- *Encryption Password* – See note below.

Note:
You may have to consult with your System Administrator to activate this function.

Traps for SNMP v1/v2/v3

Traps are used by the camera to send messages to a management system for important events or status changes.

- *Enable traps* – Check this box to activate trap reporting.
  - *Trap address* – Enter the IP address of the management server.
  - *Trap community* – Enter the community to use when sending a trap message to the management system. The default value is *public*.
- Trap Option
  - *Warm start* – A warm start SNMP trap signifies that the SNMP device, such as the camera, performs a software reload.

Click **Save** when complete.

9.3.3.4 UPnP

The **UPnP** screen enables the Universal Plug-and-Play protocol on your network devices.

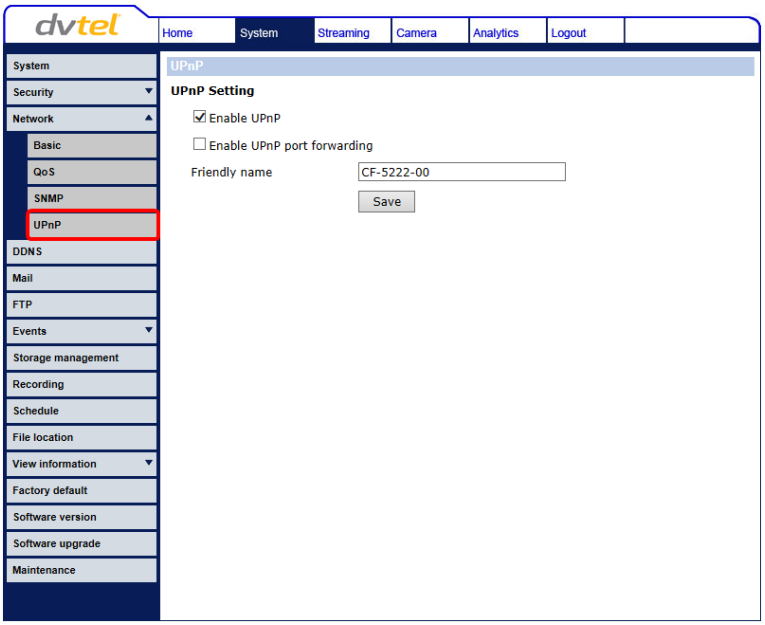


Figure 24: UPnP Screen

UPnP Setting

- *Enable UPnP* – This is the default setting. If UPnP is enabled and a camera is discovered on the LAN, the icon of the connected camera appears in **My Network Places**, allowing direct access, as seen below.

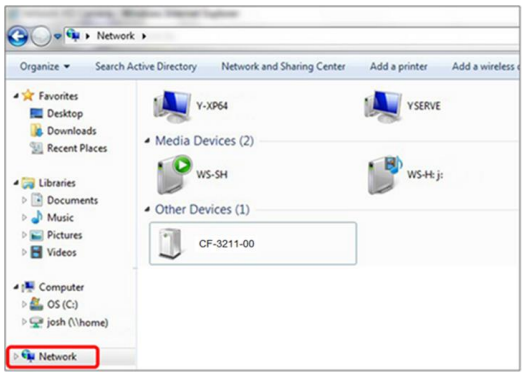


Figure 25: Direct Access to Camera with UPnP Enabled

> **Note:**
> To enable this function, make sure the UPnP component is installed on your computer. Refer to Install UPnP Components for the Windows 7, Windows 8, and Windows 8.1 procedure.

- *Enable UPnP port forwarding* – When UPnP port forwarding is enabled, the camera is allowed to open the web server port on the router automatically.

> **Note:**
> To enable this function, ensure that your router supports UPnP and is activated.

- *Friendly name* – Set the name for the camera for identification.

Click **Save** to save the settings.

9.3.4 DDNS

Dynamic Domain Name System (DDNS) allows a host name to be constantly synchronized with a dynamic IP address. This permits those using a dynamic IP address to be accessed by a static domain name. DDNS is not enabled by default.

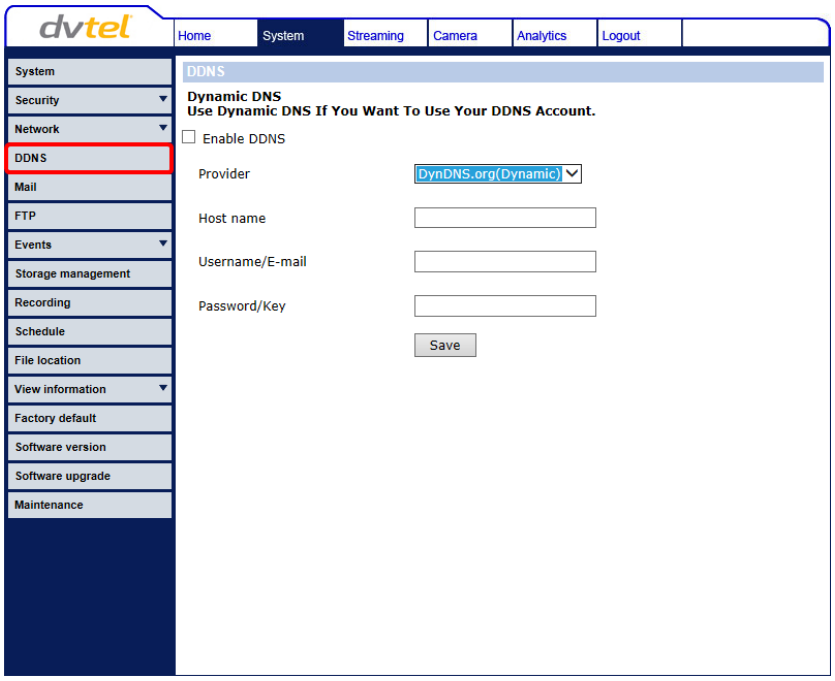


Figure 26: DDNS Screen

Enable DDNS

Check this box to enable DDNS.

- *Provider* – Select a DDNS host provider name from the drop-down list.
- *Host name* – Enter the registered domain name in the field.
- *Username/E-mail* – Enter the username or e-mail address required by the DDNS provider for authentication.
- *Password/Key* – Enter the password or key required by the DDNS provider for authentication.

Click **Save** to save the setting.

9.3.5 Mail

Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. It is a relatively simple, text-based protocol, where one or more recipients of a message are specified and the message text is transferred.

The Administrator can send an e-mail via Simple Mail Transfer Protocol (SMTP) when an alarm is triggered. Two SMTP server accounts can be configured. Enter the settings for the 1st SMTP server and 2nd SMTP server in the appropriate fields. Settings include SMTP server, server port (default port is 25), account name, password, and recipient e-mail address settings. For SMTP server details, contact your network service provider.

To use SSL encryption of the email, select the *1st SMTP SSL* or *2nd SMTP SSL* checkbox for the respective server.

Enter the sender's email address in the text box.

Click **Save** when finished.

The following screen shows the SMTP configuration.

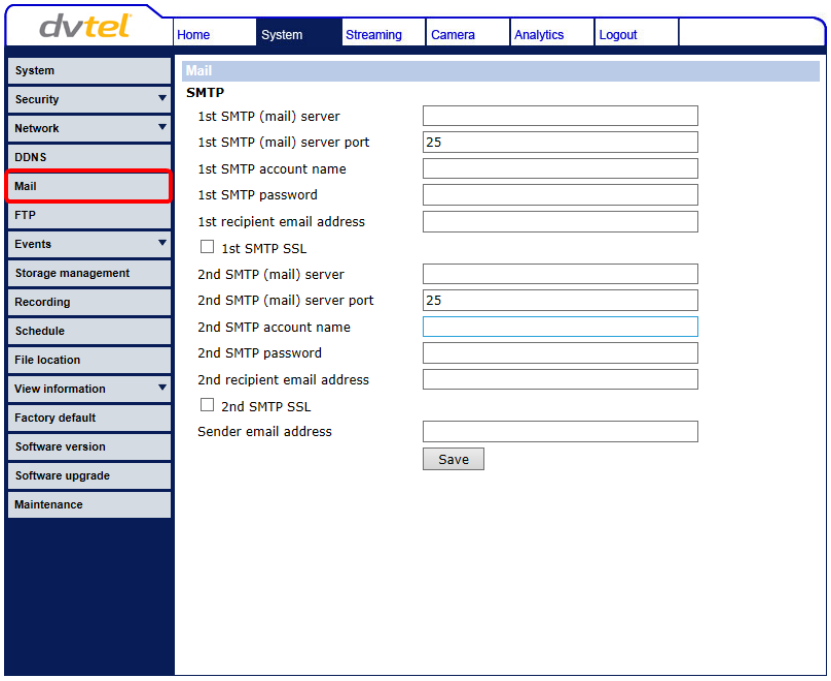


Figure 27: Mail Screen – SMTP

9.3.6 FTP

The Administrator can send an alarm message to one or two File Transfer Protocol (FTP) sites when motion is detected. For each server, enter the server IP address, server port number, user name, password, and remote folder path.

To use passive mode, select the *1st FTP passive mode* or *2nd FTP passive mode* checkbox for the respective server. In passive mode, FTP the client initiates both connections to the server, solving the problem of firewalls filtering the incoming data port connection to the client from the server.

In order to support passive mode FTP on the server-side firewall, the following communication channels must be opened:

- FTP server's port 21 from anywhere (client initiates connection)
- FTP server's port 21 to ports > 1023 (server responds to client's control port)
- FTP server's ports > 1023 from anywhere (client initiates data connection to random port specified by server)
- FTP server's ports > 1023 to remote ports > 1023 (server sends ACKs and data to client's data port)

To test the connection to the specified FTP server, click **Test** for the first or second server.

Click **Save** when finished.

The following screen shows the FTP settings.

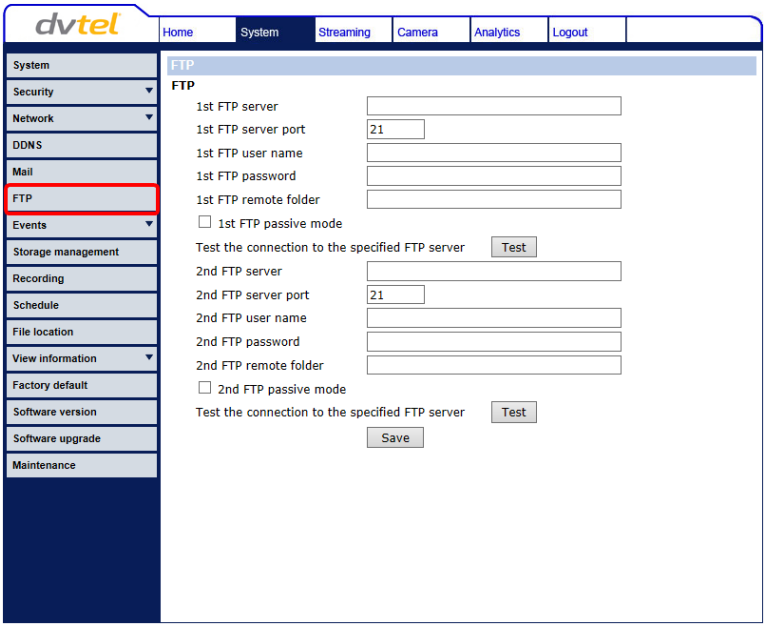


Figure 28: FTP Screen

9.3.7 Events

Clicking the **Events** tab opens two screens: **Application** and **Network Failure Detection**.

9.3.7.1 Application

The **Application** screen enables control over the input and output alarms, which are generated if an event is recognized by the system.

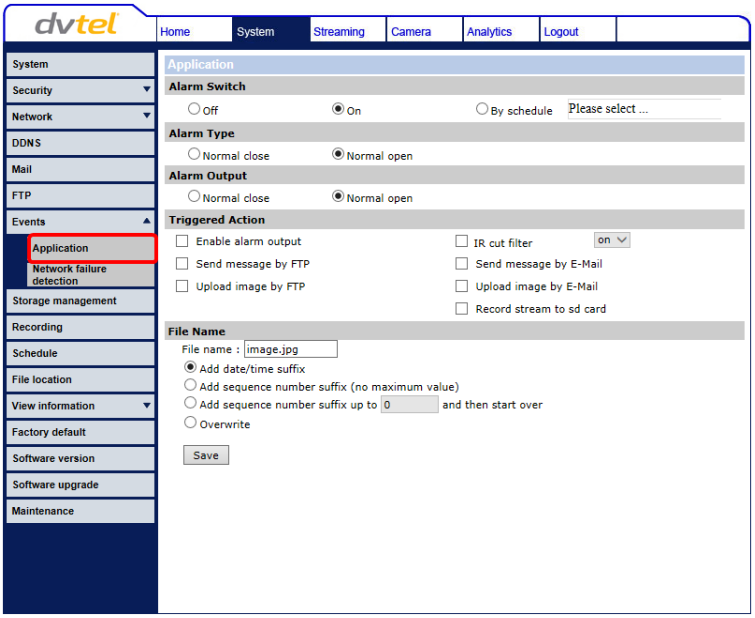


Figure 29: Events > Application Screen

9.3.7.1.1 Alarm Switch

The Administrator can select from the following options:

- Select *Off* to disable an alarm.
- Select *On* to enable an alarm (default setting).
- Select *By Schedule* to set a schedule. Then click *Please Select* to select up to 10 schedules from the drop-down list that opens. The selected schedules are displayed in the *Please Select* text box. To set a schedule, open the Schedule tab.

Click **Save** after configuring the settings.

9.3.7.1.2 Alarm Type

Select an alarm type (*Normal close* or *Normal open*) that corresponds to the alarm application. *Normal open* is the default setting. Click **Save** after configuring the settings.

9.3.7.1.3 Alarm Output

Define the normal alarm output signal as *Normal close* or *Normal open*, according to the current alarm application. *Normal open* is the default setting. Click **Save** after configuring the settings.

9.3.7.1.4 Triggered Action

The Administrator can specify various alarm actions to take when an alarm is triggered. The following options are available:

1. *Enable alarm output* – Select this checkbox to enable alarm relay output (default setting).
2. *Send Message by FTP* – Select the checkbox send an alarm message by FTP when an alarm is triggered.
3. *Upload image by FTP* – Select this box to assign an FTP site and configure the parameters shown. When an alarm is triggered, event images are uploaded to the designated FTP site. Follow these steps:
   - From the *FTP address* drop-down list, select one of the two FTP addresses to use.
   - From the *Pre-trigger buffer* and *Post-trigger buffer* drop-down lists, select the number of frames for the buffer from 1-20 frames.

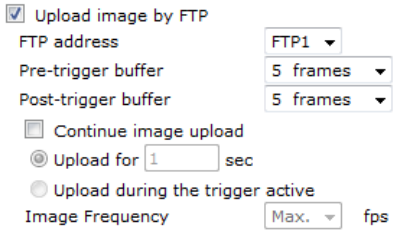


Figure 30: Triggered Action – Upload Image by FTP

   - Select the *Continue image upload* checkbox to upload an image by FTP for a defined period of time or while the trigger is active. Select one of the following options:
     - To specify the length of time for the upload, select *Upload for* and enter the number of seconds in the text box.
     - To upload while the trigger is active, select *Upload during the trigger active*.

     In the *Image Frequency* text box, from the drop-down list select the number of frames per seconds from 1-15 for the upload.

> **Note:**
> Make sure that FTP configuration has been completed. See FTP for details.

4. *IR Cut Filter* – Select this checkbox trigger an event when the IR cut filter is activated.
5. *Send Message by E-Mail* – Select the checkbox send an alarm message by e-mail when an alarm is triggered. The e-mail address is entered in the Mail screen.
6. *Upload Image by E-Mail* – Select this checkbox to assign an e-mail address for sending the image captured by a triggered alarm. The e-mail address is entered in the Mail screen.

> Note:
> This option is valid only when using MJPEG as the camera stream.

   - From the *E-Mail address* drop-down list, select one of the two e-mail addresses.

- From the *Pre-trigger buffer* and *Post-trigger buffer* drop-down lists, select the number of frames for the buffer from 1-20 frames.

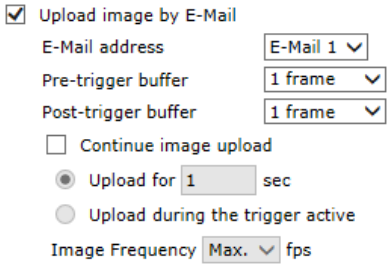


Figure 31: Triggered Action – Upload Image by E-Mail

- Check the *Continue image upload* box if you wish to upload an image by e-mail for a defined period of time or while the trigger is active. Select one of the following options:
  - To specify the length of time for the upload, select *Upload for* and enter the number of seconds in the text box.
  - To upload while the trigger is active, select *Upload during the trigger active*.

  In the *Image Frequency* text box, from the drop-down list select the number of frames per seconds from 1-15 for the upload.

> **Note:**
> Make sure that SMTP configuration has been completed. See Mail for details.

7. *Record stream to sd card* – This function is disabled in the current version and is not supported by Latitude.

Click **Save** after configuring the settings.

9.3.7.1.5 File Name

- *File Name* – Enter a file name in the field, for example *image.jpg.* The uploaded image's file name format is set in this section. Select one that meets your requirements.
  - Add date/time suffix (default setting)
    File name: imageYYMMDD_HHNNSS_XX.jpg
    Y: Year, M: Month, D: Day
    H: Hour, N: Minute, S: Second
    X: Sequence Number
  - Add sequence number suffix (no maximum value)
    File name: imageXXXXXXX.jpg
    X: Sequence Number
  - Add sequence number suffix (limited value)
    File Name: imageXX.jpg
    X: Sequence Number

    The file name suffix ends at the number being set. For example, if the setting is up to "10," the file name will start from 00, end at 10, and then start over again.
  - Overwrite
    The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Click **Save** after configuring the settings.

9.3.7.2 Network Failure Detection

The network failure detection function allows the IP camera to periodically ping another IP device within the network to detect a network failure if, for example, a video server is disconnected. It can be associated with an action of sending a notification via an alarm output, e-mail or FTP message.

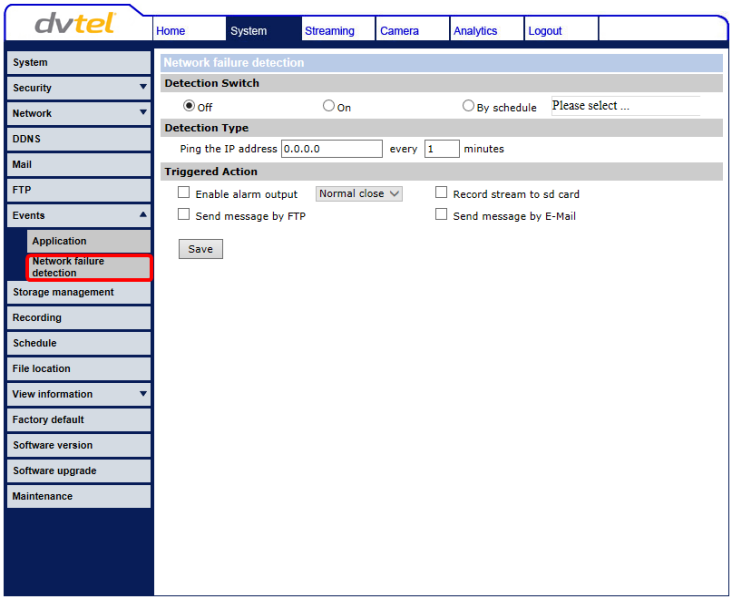


Figure 32: Events > Network Failure Detection Screen

9.3.7.2.1 Detection Switch

The Administrator can select from the following options:

- Select *Off* to disable an alarm (default setting).
- Select *On* to enable an alarm.
- Select *By Schedule* to set a schedule. Then click *Please Select* to select up to 10 schedules from the drop-down list that opens. The selected schedules are displayed in the *Please Select* text box. To set a schedule, open the Schedule tab.

Click **Save** after configuring the settings.

9.3.7.2.2 Detection Type

In the text box, enter the IP address to ping and the time interval (in minutes) between pings. Click **Save** after configuring the settings.

9.3.7.2.3 Triggered Action

The Administrator can specify various alarm actions to be taken when an alarm is triggered. The following options are available:

1. *Enable alarm output* – Select this checkbox to enable alarm relay output. From the drop-down list, select *Normal open* or *Normal close*.
2. *Send Message by FTP* – Select the checkbox send an alarm message by FTP when an alarm is triggered.

> **Note:**
> Make sure that FTP configuration has been completed. See FTP for details.

3. *Record stream to sd card* – This function is disabled in the current version and is not supported by Latitude.
4. *Send Message by E-Mail* – Select the checkbox send an alarm message by e-mail when an alarm is triggered.

> **Note:**
> Make sure that SMTP configuration has been completed. See Mail for details.

Click **Save** after configuring the settings.

9.3.8 Storage Management

This function is not supported and cannot be used.

9.3.9 Recording

This function is not supported and cannot be used.

9.3.10 Schedule

The **Schedule** screen is used to set schedules for recording of events triggered in the Event > Application and Event > Network Failure Detection screens.

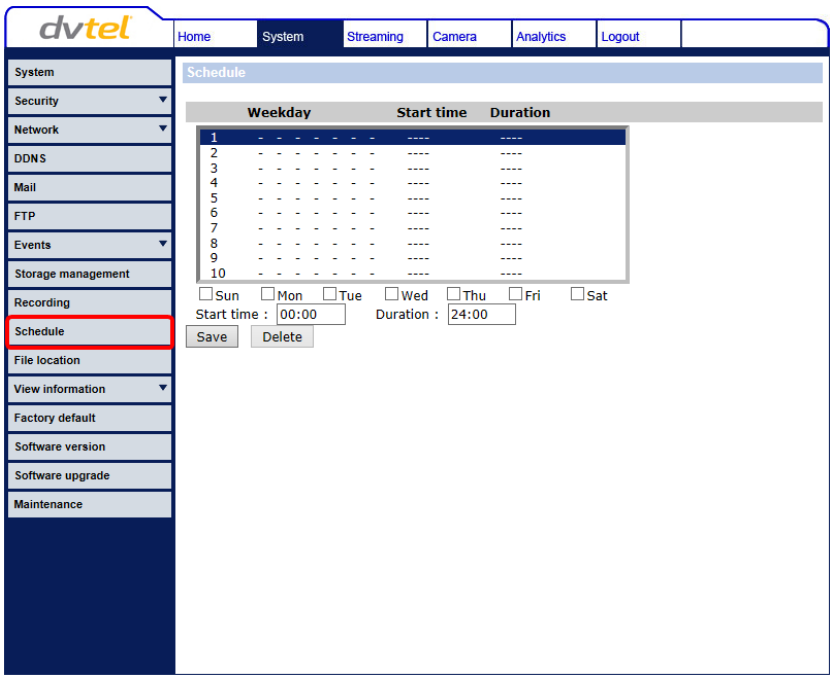


Figure 33: Schedule Screen

The functions in this tab allow administrators to create customized schedules for the camera that uses this option. If a schedule exists, the administrator can apply that schedule to this camera using the available drop-down list.

To create a new schedule or edit an existing schedule

1. Click the appropriate checkboxes relating to the days of the week (Sun, Mon, Tue, Wed, Thu, Fri and Sat) to create a schedule.
2. Set *Start time* (for example, 09:00) and *Duration* (for example, 4:00 hours).
3. Click **Save** to apply the newly created schedule to the camera.

To remove a schedule

1. Select the schedule by clicking the line.
2. Click **Delete** to remove the schedule.

9.3.11 File Location

From the **File Location** screen, specify a storage location for snapshots and web recordings. The default setting is: C:\. After confirming the setting, click **Save** to save the snapshots and recordings in the designated location.

Note:
Make sure the selected file path contains valid characters.

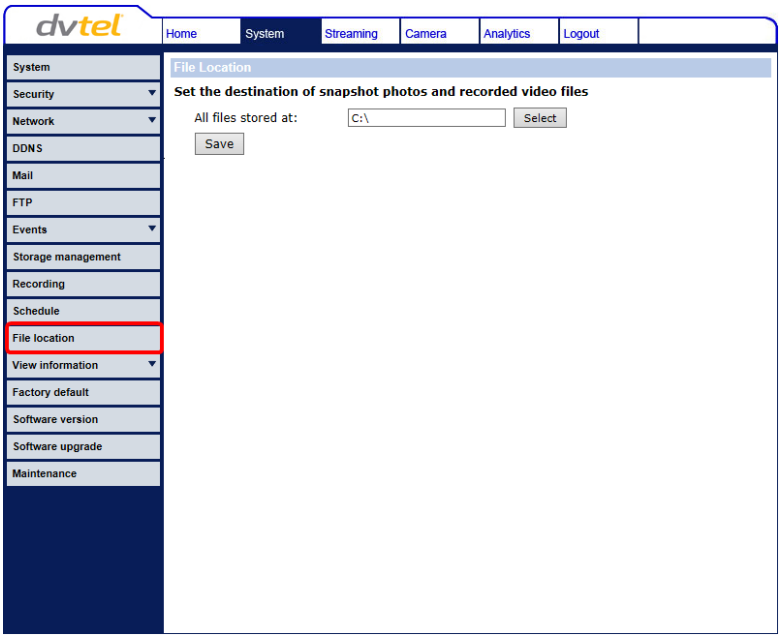


Figure 34: File Location Screen

9.3.12 View Information

Clicking the **View Information** tab in the **System** screen opens a drop-down list with the following tabs: **Log File**, **User Information**, and **Parameters**.

Related Links

- Log File
- User Information
- View Parameters

9.3.12.1 View Log File

The log file provides information about connections after system boot-up. Click **Log file** to view the system log file. The **System log** screen opens.

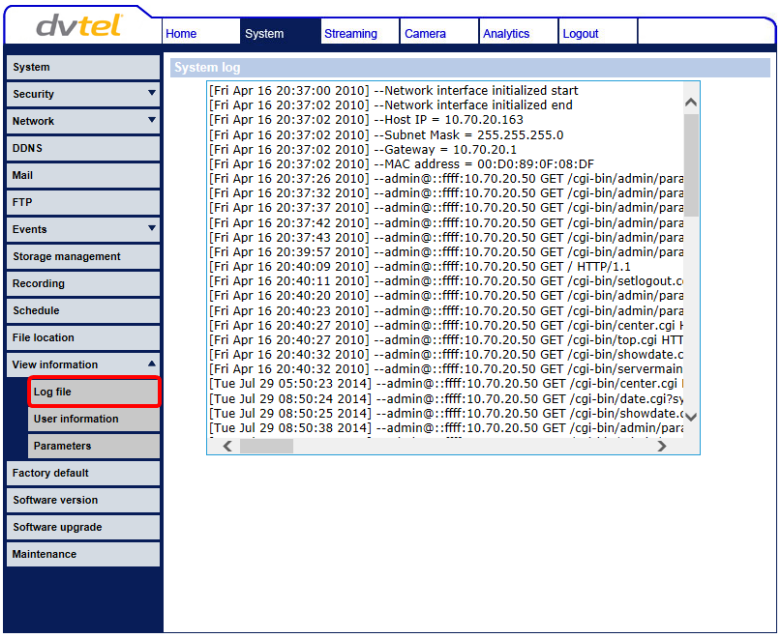


Figure 35: System Log Screen

9.3.12.2 User Information

The Administrator can view each user's login information and privileges in the **User information** screen shown below.

View User Login Information

Click **get user information** to see each user's details. For example: *admin: admin*. This indicates that the user's login username is *admin* and the password is *admin*.

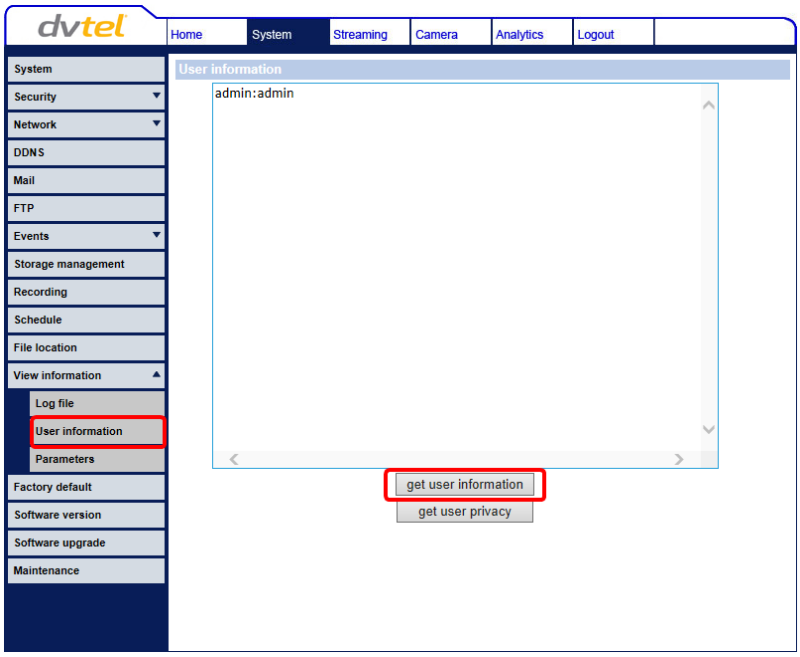


Figure 36: View Information > User Information Screen

View User Privilege

Click **get user privacy** to view each user's privileges.

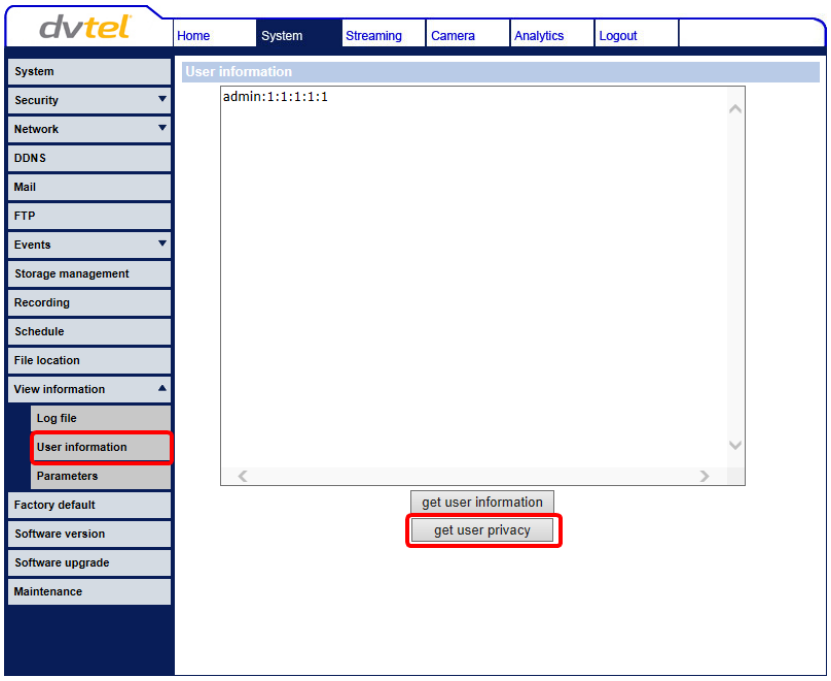


Figure 37: View Information > User Information – Get User Privacy Screen

In Figure 37, the user *Admin* is granted privileges of I/O access, Camera control, Talk, Listen, and Analytics.

Note:

User privileges are defined in the Security > User screen. The example above shows the maximum privileges that can be granted. It is however, dependent on the specific user's security level.

9.3.12.3 View Parameters

The **Parameter** screen enables viewing all of the system's parameter settings (not the analytic parameters).

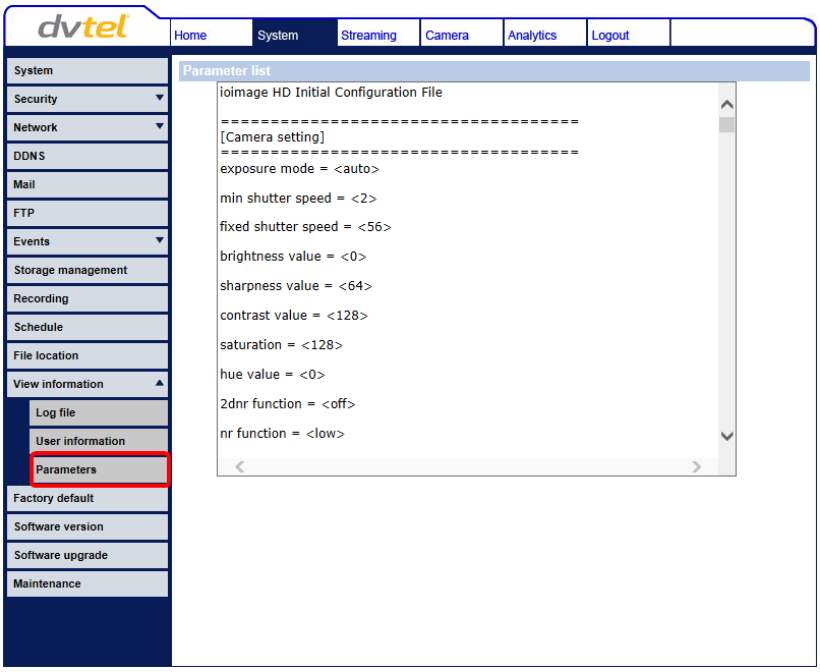


Figure 38: Parameter List Screen

Note:

Slide the sidebar located on the right of the screen to view the entire list of parameters.

9.3.13 Factory Default

The **Factory default** screen is shown below. Follow the instructions to reset the camera system settings to factory default settings if needed.

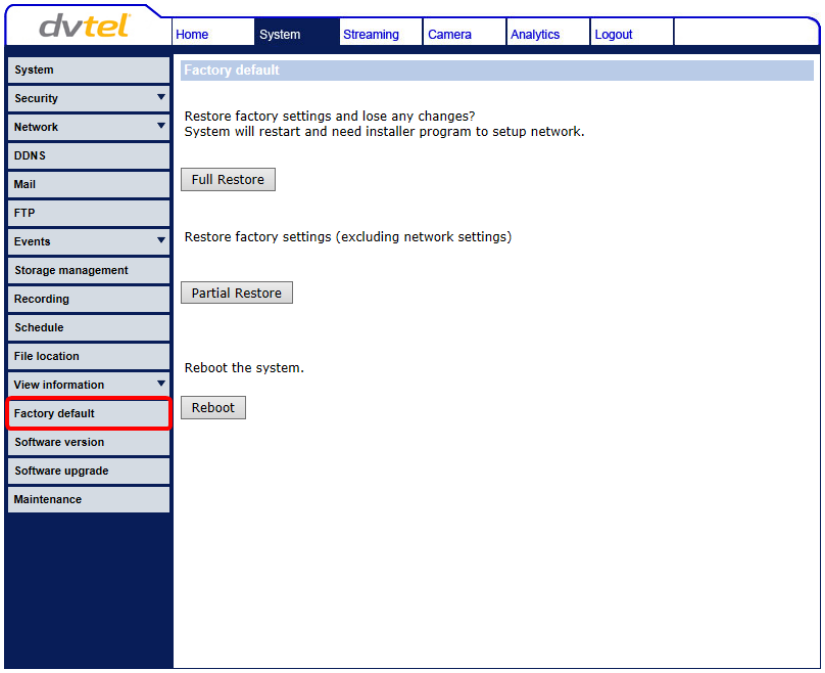


Figure 39: Factory Default Screen

Full Restore

Click **Full Restore** to restore the factory default settings of the camera system. The system restarts in 30 seconds.

> **Note:**
> The IP address and all other settings will be restored to factory default settings.

Partial Restore

Click **Partial Restore** to restore the factory default settings of the camera system, but save the network settings. The system restarts in 30 seconds.

Reboot

Clicking **Reboot** restarts the system without changing current settings.

> **Note:**
> Analytics firmware is stored in a separate file than the camera system firmware. To backup and restore the analytics firmware version, see Analytics > Backup & Restore.

9.3.14 Software Version

The current version of the camera system software is displayed in the **Software version** screen.

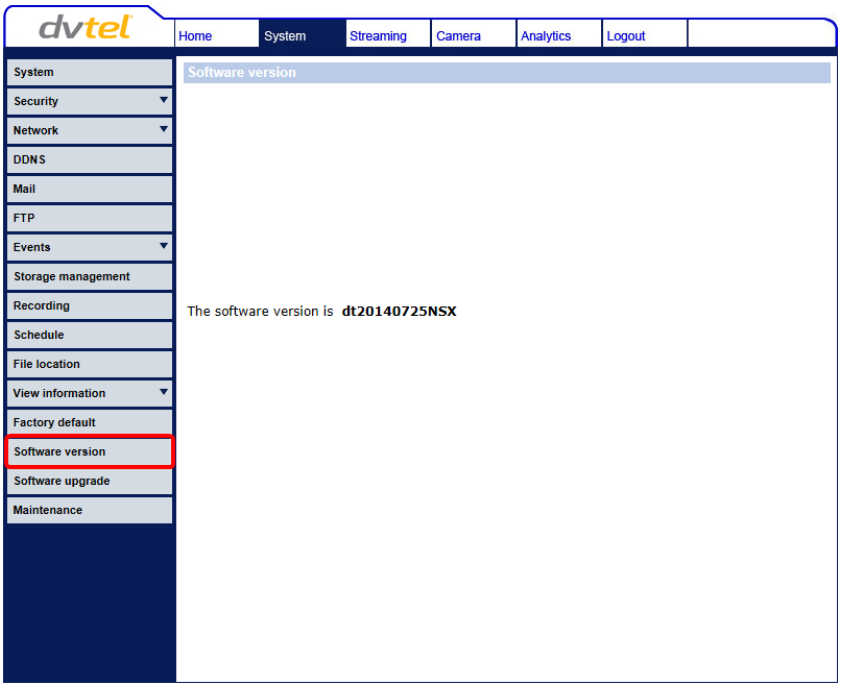


Figure 40: Software Version Screen

Note:

Analytics firmware is stored in a separate file than the camera system software. To view the analytics firmware version, see Analytics > Firmware.

9.3.15 Software Upgrade

Select the **Software Upgrade** tab to select binary files to upload and upgrade. The **Upgrade** screen is shown below.

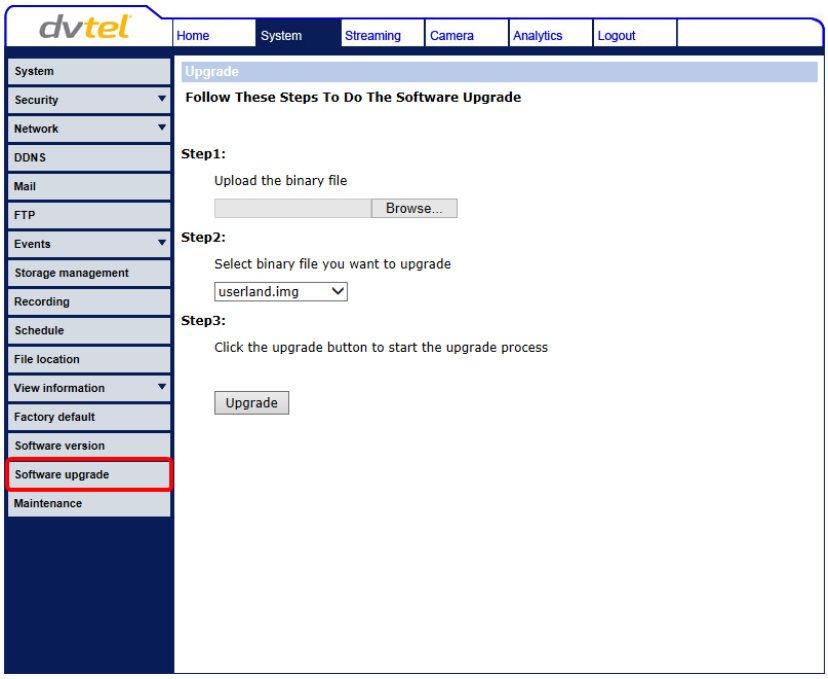


Figure 41: Software Upgrade Screen

Note:

Make sure that the software upgrade file is available before performing a software upgrade.

Note:

Analytics firmware is stored in a separate file than the camera system software. To upgrade the analytics firmware version, see Analytics > Firmware.

To upgrade the software

1. In the *Step 1* text box, click **Browse** and select the binary file to be uploaded, for example, `uImage+userland.img`.

   Note:

   Do not change the upgrade file name or the system will fail to find the file.

2. From the drop-down list of binary files in *Step 2*, select the file to upgrade. In the above example `uImage+userland.img` is selected.
3. Click **Upgrade**. The system verifies that the upgrade file exists and begins to upload the file. The upgrade status bar is displayed on the screen. After the upgrade process has finished, the **Home** page is displayed.

Warning:

Do not unplug power or change the screen while upgrading software.

Avertissement:

Ne débranchez pas l'alimentation pendant la mise à niveau du logiciel.

9.3.16 Maintenance

You can export configuration files to a specified location and retrieve data by uploading an existing configuration file to the camera.

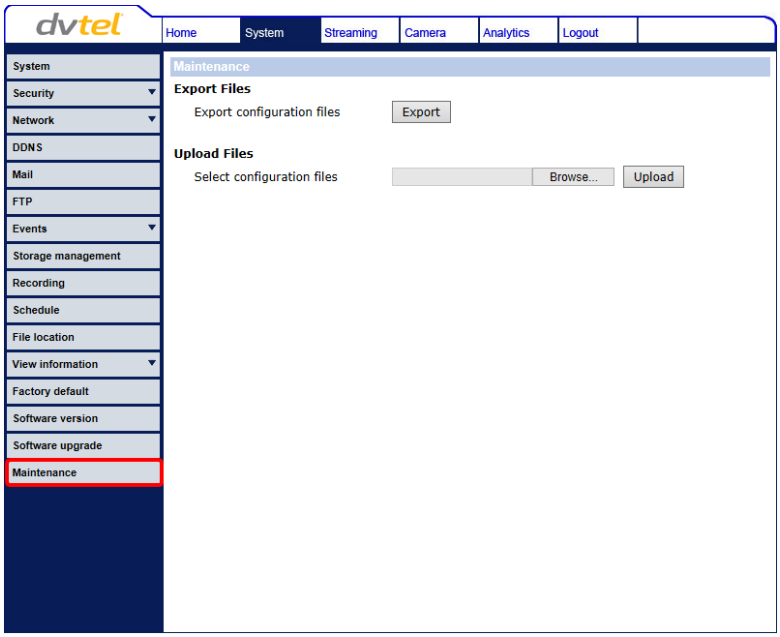


Figure 42: Maintenance Screen

Warning:

Do not unplug power while changing file names.

Avertissement:

Ne débranchez pas l'alimentation pendant la modification des noms de fichiers.

Export

You can save system settings by exporting the configuration file (`.bin`) to a specified location for future use. Click **Export** and the popup window **File Download** appears as shown below.

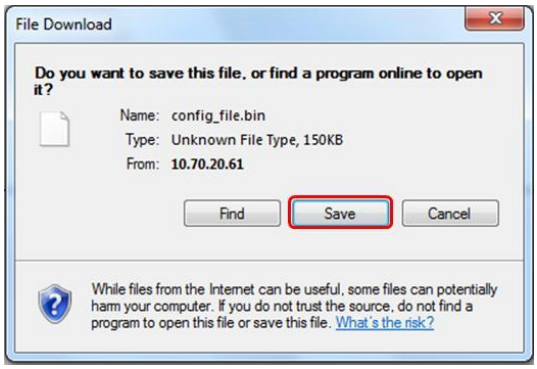


Figure 43: File Download Screen

Click **Save** and specify a location to save the configuration file.

Upload

To copy an existing configuration file to the camera, click **Browse** to select the configuration file, and then click **Upload** to upload the file.

Note:

The camera firmware and the analytics firmware use separate configuration files. For analytic firmware configuration file, see Analytics > Backup & Restore.

9.4 Video and Audio Streaming Settings

Select the **Streaming** tab in the navigation bar at the top of the screen to display the configurable video and audio selections in the sidebar. The Administrator can configure specific video resolution, video compression mode, video protocol, audio transmission mode, etc. Further details of these settings are specified in the following sections.

The following video formats are supported:

- MJPEG
- H.264

Related Links

- Video Format
- Video Compression
- Video OCX Protocol
- Video Frame Rate
- Audio

9.4.1 Video Format

From the **Video Format** screen, you can configure the following settings:

- Video Resolution
- GOV Settings
- H.264 Profile

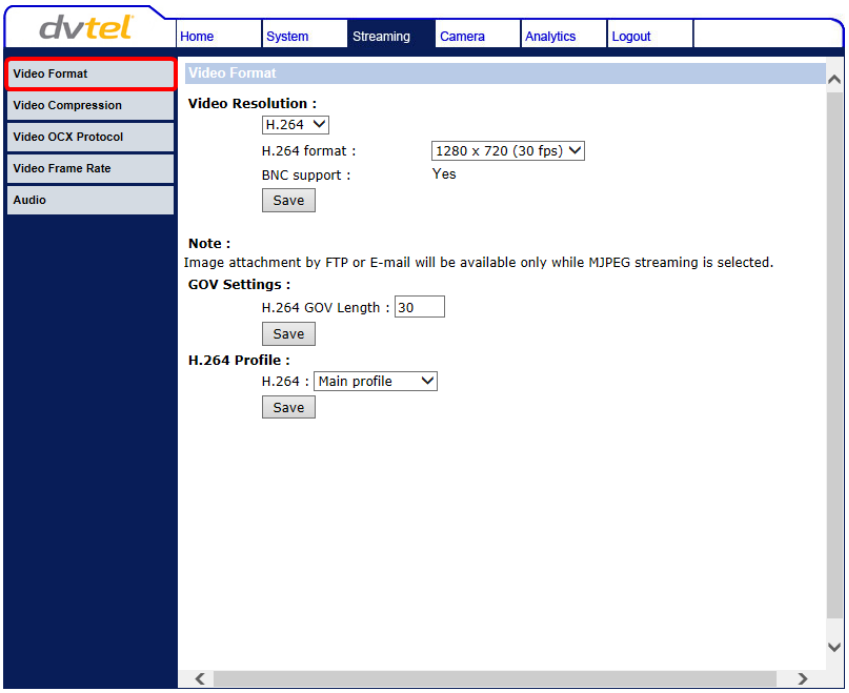


Figure 44: Streaming > Video Format Screen

9.4.1.1 Video Resolution

The ioimage HD camera supports H.264/MJPEG streaming for resolutions up to 1080p on the CF-5222 and 720p on the CF-5212. The default setting for CF-5222 is *1920 x 1080*. The default setting for CF-5212 is *1280 x 720*.

Following are the supported resolutions for each model:

CF-5222		CF-5212	
PAL	**NTSC**	**PAL**	**NTSC**
1920 x 1080	1920 x 1080		
1280 x 1024	1280 x 1024	1280 x 720	1280 x 720
720 x 576	720 x 480	720 x 576	720 x 480

9.4.1.2 GOV Settings

You can set the GOV length to determine the frame structure (I-frames and P-frames) in a video stream for saving bandwidth. The setting range is from *2* to *64*. A longer GOV decreases the frequency of I-frames. The default setting is *30.* Click **Save** to confirm the GOV setting.

9.4.1.3 H.264 Profile

The H.264 standard defines 21 sets of capabilities. These are referred to as profiles and they target specific classes of applications. In the security industry, the most common are as follows:

- **Baseline Profile (BP)**
  Primarily for low-cost applications that require additional data loss robustness, *Baseline Profile* is used in some videoconferencing and mobile applications. This is the most common profile used in IP security cameras due to the low computational cost of processing the video using this profile.

- **Main Profile (MP)**
  This profile provides improved picture quality at reduced bandwidths and storage costs and is becoming more common as the camera processors (DSPs) become more able to handle the processing load. *Main Profile* can save 10-30% over *Baseline*. This is the default setting.
- **High Profile (HP)**
  High Profile is the primary profile for HD broadcast and Blu-ray HD disc media applications. It can save 10-30% of the storage cost over *Main Profile*. However, it may also increase video latency, depending on the stream structure. ioimage HD models default to the *Main Profile* to provide the best trade-off between storage size and video latency.

Click **Save** to confirm the settings.

9.4.2 Video Compression

From the **Video Compression** screen, you can specify MJPEG and H.264 compression settings.

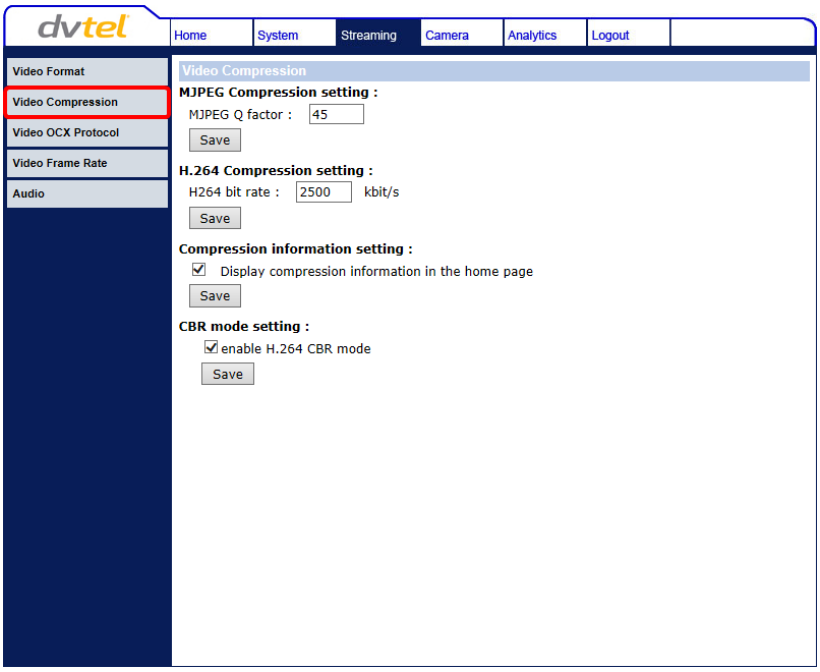


Figure 45: Streaming > Video Compression Screen

MJPEG Compression Setting

A higher value implies higher bit rates and higher visual quality. The default setting of the MJPEG Q factor is *35*. The setting range is from *1* to *70*. Click **Save** to confirm the setting.

H.264 Compression Setting

The default setting of H.264 is *4096* kbps. The setting range is from *64* to *8192* kbps. Click **Save** to confirm the setting.

Compression Information Setting

Select the checkbox to display compression information on the **Home** page. The default setting is *Display compression information in the home page*. Click **Save** to confirm the setting.

CBR Mode Setting

If available bandwidth is limited, check *enable H.264 CBR mode* to use Constant Bit Rate. The default setting is *enable H.264 CBR mode*. To operate the camera in Variable Bit Rate (VBR) mode, uncheck the CBR checkbox. Click **Save** to confirm the setting.

Note:
CBR mode affects image quality.

9.4.3 Video OCX Protocol

From the **Video OCX Protocol** screen, you can select various protocols for streaming media over the network. In the case of multicast networking, select *Multicast mode*.

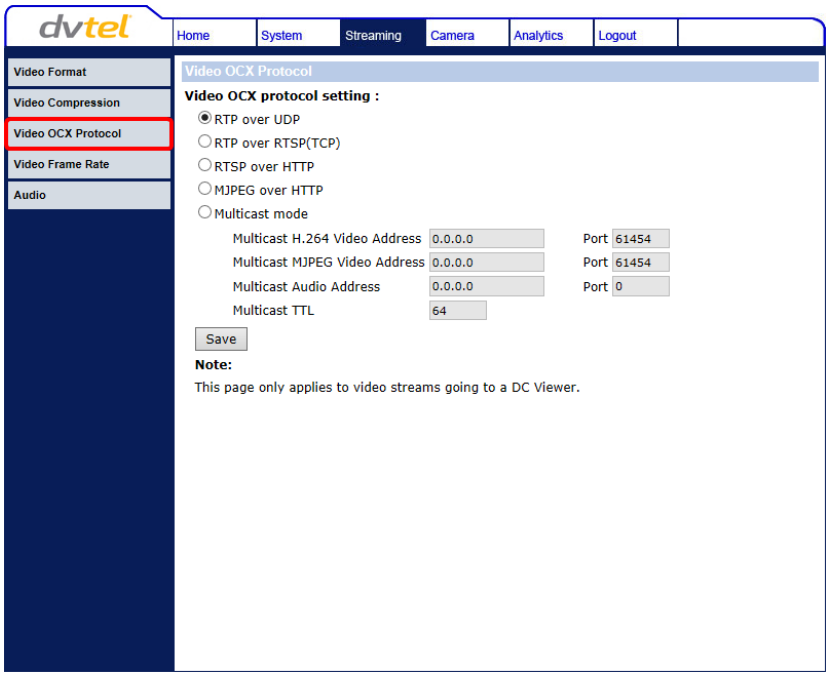


Figure 46: Streaming > Video OCX Protocol Screen

Video OCX protocol setting options include:

- *RTP over UDP* (default setting)
- *RTP over RTSP (TCP)*
- *RTSP over HTTP*
- *MJPEG over HTTP*
- *Multicast mode* – Enter in each field all required data, including *Multicast H.264 Video Address* and *Port, Multicast MJPEG Video Address* and *Port, Multicast Audio Address* and *Port,* and *Multicast TTL*. The default Multicast TTL (time-to-live) setting is *1*, which prevents multicast datagrams from being forwarded beyond a single sub-network.

Click **Save** to confirm the settings.

Note:
This screen applies only to video streams that are sent to the DCViewer.

9.4.4 Video Frame Rate

From the **Video Frame Rate** screen, you can specify the frames per second (fps) for each video compression format.

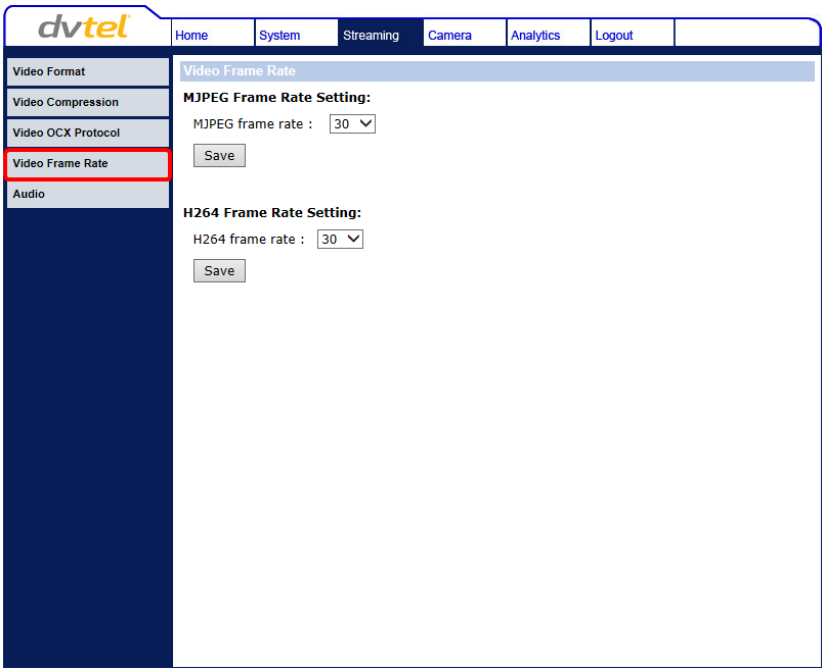


Figure 47: Streaming > Video Frame Rate Screen

MJPEG/H.264 Frame Rate Setting

- The default setting of the MJPEG frame rate is *30* fps in NTSC and *25* fps in PAL.
- The default setting of the H.264 frame rate is *30* fps in NTSC and *25* fps in PAL The setting range is from *1* to *30* in NTSC and *1* to *25* in PAL. Settings are:
  - PAL: *1, 5, 13,* and *25* fps
  - NTSC: *1, 2, 3, 6, 7.5, 10, 15,* and *30* fps

Click **Save** to confirm the settings.

9.4.5 Audio

From the **Audio** screen you can select the Transmission Mode, Server Gain, and Bit Rate.

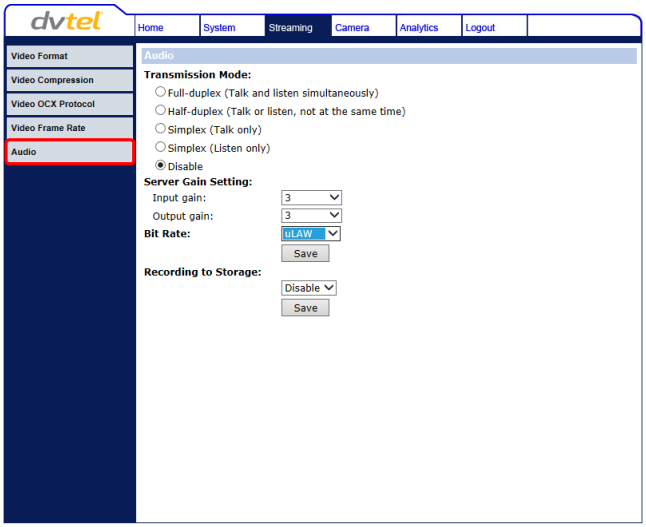


Figure 48: Audio Screen

Transmission Mode

- *Full-duplex (Talk and listen simultaneously)* – In this mode, the local and remote sites can communicate with each other simultaneously, i.e. both sites can speak and be heard at the same time. This is the default setting.
- *Half-duplex (Talk or listen, not at the same time)* – In this mode, the local or remote site can only talk or listen to the other site at one time.
- *Simplex (Talk only)* – In this mode, the local/remote site can only talk to the other site.
- *Simplex (Listen only)* – In this mode, the local/remote site can only listen to the other site.
- *Disable* – Select this option to turn off the audio transmission function.

Server Gain Setting

Set the audio input/output gain levels for sound amplification. Audio gain values are adjustable: input from *1* to *10* and output from *1* to *6*. Sound will be turned off if the audio gain is set to *Mute*. The default setting is *3* for the input gain and output gain.

Bit Rate

Audio transmission bit rates include *16 kbps (G.726), 24 kbps (G.726), 32 kbps (G.726), 40 kbps (G.726), µLAW (G.711)* and *ALAW (G.711*). Both µLAW and ALAW signify 64 kbps, but in different compression formats. A higher bit rate enables higher audio quality, but requires higher bandwidth. The default setting is *uLAW*.

Note:
Latitude does not support G.726 bit rates.

Click **Save** to confirm the settings.

Recording to Storage

This function is not supported and cannot be used.

9.5 Camera-Related Settings

Note:

The user interface displayed on the **Camera** tab depends whether *Shutter WDR* is enabled in the **Camera** tab.

9.5.1 Camera Settings with Shutter WDR Enabled

From the **Camera** tab, the administrator can adjust the following camera settings when *Shutter WDR* is set to *On* (enabled):

- Exposure
- Picture Adjustment
- IR Function
- 3DNR
- 2DNR
- TV System
- Shutter WDR

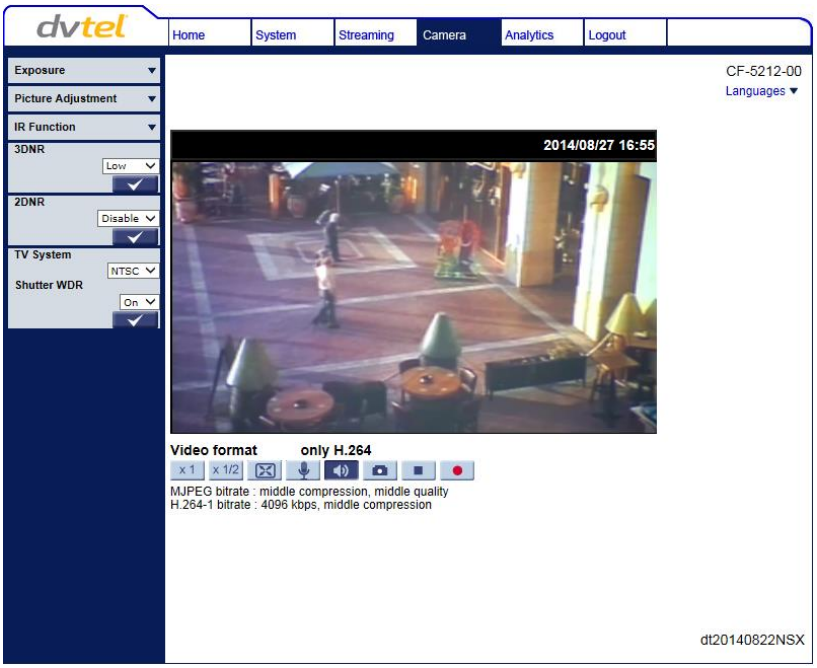


Figure 49: Camera Tab with Shutter WDR On

Note:

The user interface displayed above in the **Camera** tab is with *Shutter WDR* enabled.

9.5.1.1 Exposure

The exposure is the amount of light received by the image sensor and is determined by the amount of exposure by the sensor (shutter speed), and other exposure parameters.

Administrators may either allow the camera to automatically select an exposure level using a programmed algorithm or set a manual level. Even in *Auto Mode*, a minimum shutter speed may be set from the drop-down list to ensure a maximum level of exposure. The smaller the number (the higher the shutter speed) that the administrator selects, the lower the exposure level and vice versa.

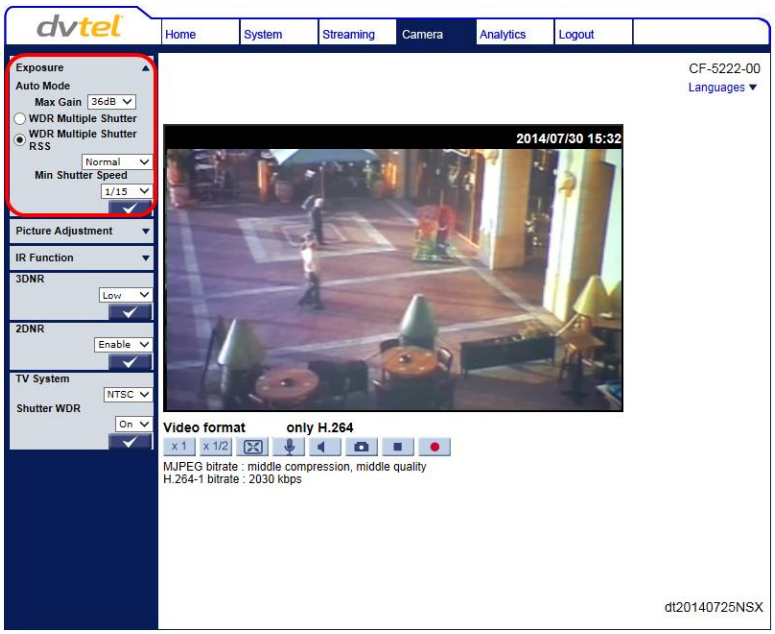


Figure 50: Camera > Exposure Screen with Shutter WDR On

Two modes of operation are available: *WDR Multiple Shutter* and *WDR Multiple Shutter RSS*.

- *WDR Multiple Shutter* (True WDR) – The camera's shutter speed works automatically to achieve a consistent video output level. You can select a suitable shutter speed according to the environmental luminance.
- *WDR Multiple Shutter RSS* – This setting is recommended when flickering occurs in indoor applications where fluorescent lighting is used. The shutter speed decreases in order to compensate for decreased ambient lighting.

To configure exposure settings

1. From the *Auto Mode Max Gain* drop-down list, select the maximum gain in 3db steps from *Off* to *72dB*. Increasing the gain lightens dark pictures resulting from low-level lighting. The default setting is *36dB*.
2. Select one of the following WDR Multiple Shutter settings: WDR Multiple Shutter or WDR Multiple Shutter RSS.

- *WDR Multiple Shutter* – The camera's shutter speed works automatically to achieve a consistent video output level. Two shutter speeds are available. Select the one that provides the ideal image quality according to the environmental luminance. This setting is *Off* by default.
    - From the drop-down list, select *Normal* or *WDR First*.
        - *Normal* – Select this setting for low-light conditions.
        - *WDR First* – This mode is recommended for indoor environments with mixed lighting sources where the main source is indoor lighting and natural light enters the scene through windows and other exposed areas. The setting reduces the overexposure in the area with natural lighting.
    - From the *Min Shutter Speed* drop-down list, select a shutter speed from *1/12* to *1/425* sec (PAL) or *1/15* to *1/500* sec (NTSC). The default setting is *1/12* (PAL) or *1/15* (NTSC). The following table displays the options.

WDR Multiple Shutter Min Shutter Speed		WDR Multiple Shutter Min Shutter Speed	
PAL	**NTSC**	**PAL**	**NTSC**
1/425	1/500	1/100	1/100
1/300	1/350	1/75	1/90
1/215	1/250	1/50	1/60
1/150	1/180	1/25	1/30
1/120	1/125	1/12	1/15

    - Select <√> to confirm the new setting.
- *WDR Multiple Shutter RSS*
    - From the drop-down list, select *Normal* or *WDR First*.
        - *Normal* – Select this setting for low-light conditions.
        - *WDR First* – This mode is recommended for indoor environments with mixed lighting sources where the main source is indoor lighting and natural light enters the scene through a window or other exposed areas. The setting reduces the overexposure in the area with natural lighting.

- From the *Min Shutter Speed* drop-down list, select a shutter speed. A fixed exposure is set, while other parameters can change. The range is from *1* to *1/500* sec (NTSC) or *1/1.5* to *1/425* sec (PAL). The following table displays the options.

WDR Multiple Shutter RSS Min Shutter Speed		WDR Multiple Shutter RSS Min Shutter Speed	
PAL	**NTSC**	**PAL**	**NTSC**
1/425	1/500	1/100	1/100
1/300	1/350	1/75	1/90
1/215	1/250	1/50	1/60
1/150	1/180	1/25	1/30
1/120	1/125	1/12	1/15

- Select <√> to confirm the new setting.

9.5.1.2 Picture Adjustment

Adjustment of some qualities of the video is made possible by selecting *Picture Adjustment* in the **Camera** tab. Brightness, Sharpness, Contrast, Saturation and Hue may all be adjusted via drop-down lists from this window, as shown below.

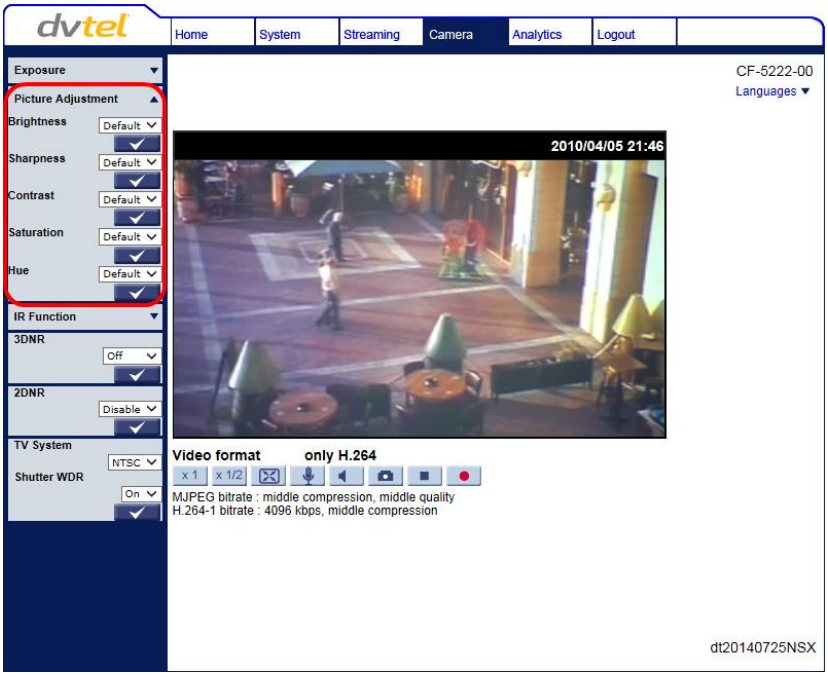


Figure 51: Camera > Picture Adjustment Screen with Shutter WDR On

9.5.1.2.1 Brightness

You can adjust the image's brightness by adjusting this parameter. Select from the range between *+1* to *+13*. To increase video brightness, select a larger number. The default setting is *Default (0)*. Select <√> to confirm the new setting.

9.5.1.2.2 Sharpness

Increasing the sharpness level can make the image look sharper, especially enhancing the object's edge. Select from the range between *-15* to *+10* in 1dB steps. The default setting is *0*. Select <√> to confirm the new setting.

9.5.1.2.3 Contrast

Camera image contrast level is adjustable: select from a range of *-13* to *+12* in 1dB steps. The default setting is *0*. Select <√> to confirm the new setting.

9.5.1.2.4 Saturation

Camera image saturation level is adjustable: select from a range of *-12* to *+13*. The default setting is *0*. Select <√> to confirm the new setting.

9.5.1.2.5 Hue

Camera image hue level is adjustable: select from a range of *+1* to *+12*. The default setting is *Default (0)*. Select <√> to confirm the new setting.

9.5.1.3 IR Function

The IR Function setting activates the IR Cut (IRC) filter for electronic day/night operation. The day/night IRC switching mechanism operates according to the ambient light level.

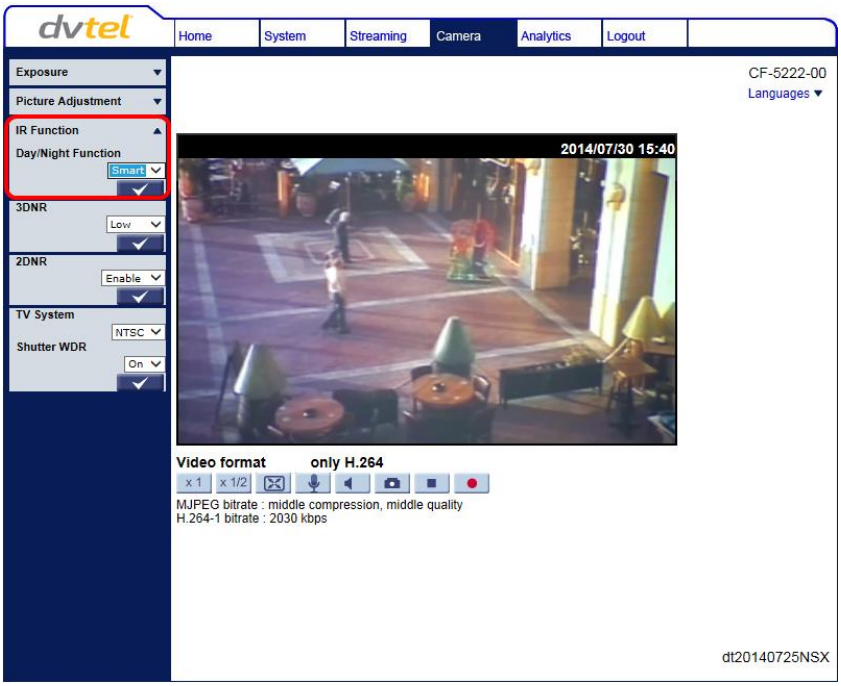


Figure 52: Camera > IR Function Screen with Shutter WDR On

From the drop-down list, select one of the four settings:

- *Auto* – The camera converts from Day mode (color) to Night mode (monochrome) automatically at nighttime or in low light conditions. When there is sufficient light, the camera converts automatically from Night mode to Day mode. This is the default setting.
- *Night* – Activates IR mode (puts camera into monochrome/Night mode).
- *Day* – Deactivates IR mode (puts camera into color/Day mode).
- *Smart* – Default mode. Smart mode enhances monochrome/Night mode stability when IR illumination is dominant and keeps the camera from switching between Day and Night modes. In this mode, the IR Cut filter is on (i.e. monochrome/Night mode) when the IR LED illuminator also is activated. This prevents the camera from returning to color/Day mode.

Select <√> to confirm the new setting.

9.5.1.4 3DNR

3DNR provides superior noise reduction and is recommended for use in in extra low-light conditions. It is especially useful for reducing blur with moving objects. There are three options for 3D Noise Reduction (3DNR). A higher level of 3DNR generates relatively enhanced noise reduction. From the drop-down list, select *Low, Middle* or *High*. The default setting *Low*. Select <√> to confirm the new setting.

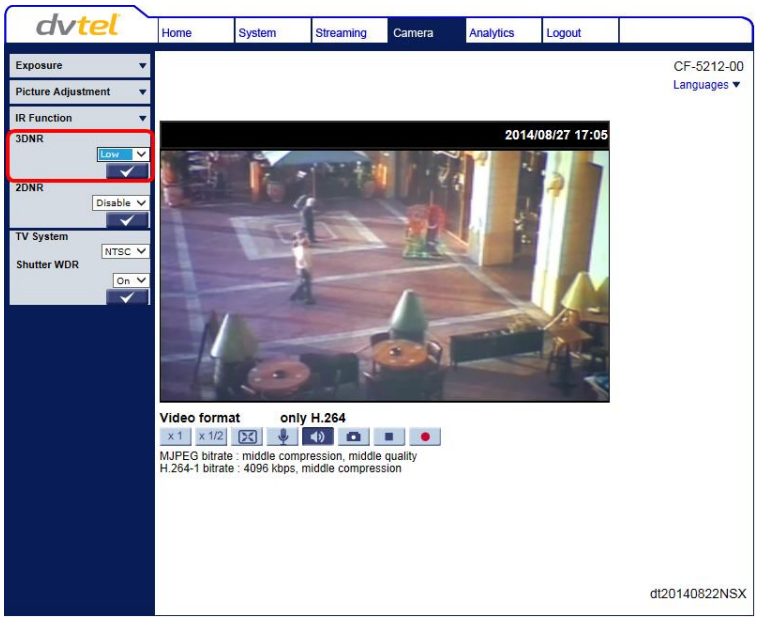


Figure 53: Camera > 3DNR Screen with Shutter WDR On

9.5.1.5 2DNR

The 2DNR Noise Reduction function analyzes pixel by pixel and frame by frame to eliminate environmental noise and deliver optimized image quality, especially in low-light conditions. From the drop-down list, select *Disable* or *Enable.* The default setting *Disable.* Select <√> to confirm the new setting.

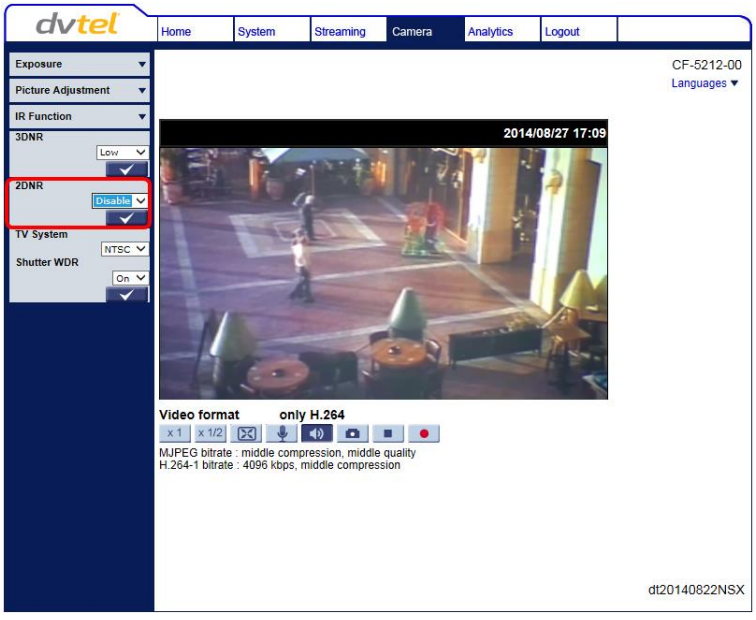


Figure 54: Camera > 2DNR Screen with Shutter WDR On

9.5.1.6 TV System

Select the video format that matches your TV system: *25 fps* (PAL*)* or *30 fps* (NTSC). The default setting is *NTSC*. Select <√> to confirm the new setting.

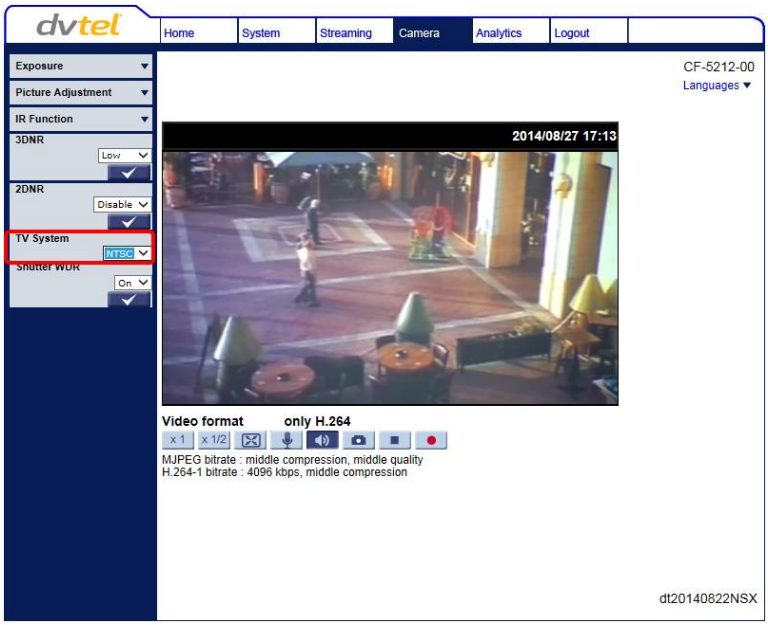


Figure 55: Camera > TV System Screen with Shutter WDR On

Note:

After changing the video format, the camera restarts automatically.

9.5.1.7 Shutter WDR

The Shutter WDR (Wide Dynamic Range) function resolves high contrast or changing light issues in order to enhance the video display. The camera supports multi-exposure WDR, which is implemented by using a combination of slow- and fast-exposure shutters. The camera uses an algorithm to determine the optimal mix of light and dark regions within the scene from the two shutters in order to adjust the wide dynamic range of the scene.

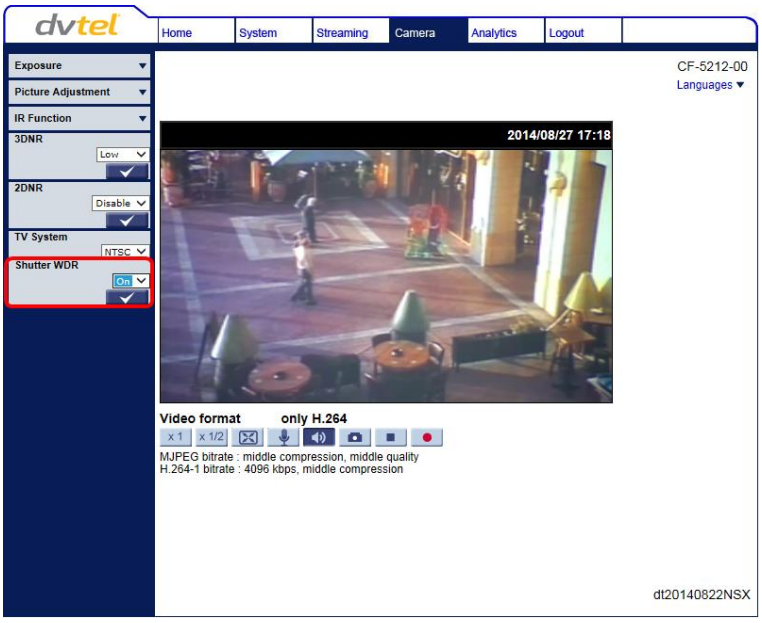


Figure 56: Camera > Shutter WDR Screen with Shutter WDR On

The WDR is selectable between *On* or *Off:*

- When *On* is selected, the image has a wide dynamic range, so that the IP camera can capture a greater scale of brightness.
- Selecting *Off* disables this function. This is the default setting.

Select <√> to confirm the new setting.

Note:

If you select *Off* as the *Shutter WDR* setting, the camera restarts automatically and a different user interface is displayed for the **Camera** tab. See the next section.

Press <√> to confirm the new setting.

9.5.2 Camera Settings with Shutter WDR Disabled

From the **Camera** tab, the administrator can adjust the following camera settings when *Shutter WDR* is set to *Off* (disabled):

- Exposure
- Picture Adjustment
- IR Function
- Backlight
- Gamma WDR
- 3DNR
- 2DNR
- TV System
- 3DNR
- Shutter WDR

Note:

The user interface displayed below in the **Camera** tab is with *Shutter WDR* disabled.

9.5.2.1 Exposure

The CF-5212/CF-5222 camera supports the setting of different parameters for various exposure modes that control the amount of light received by the image sensor.

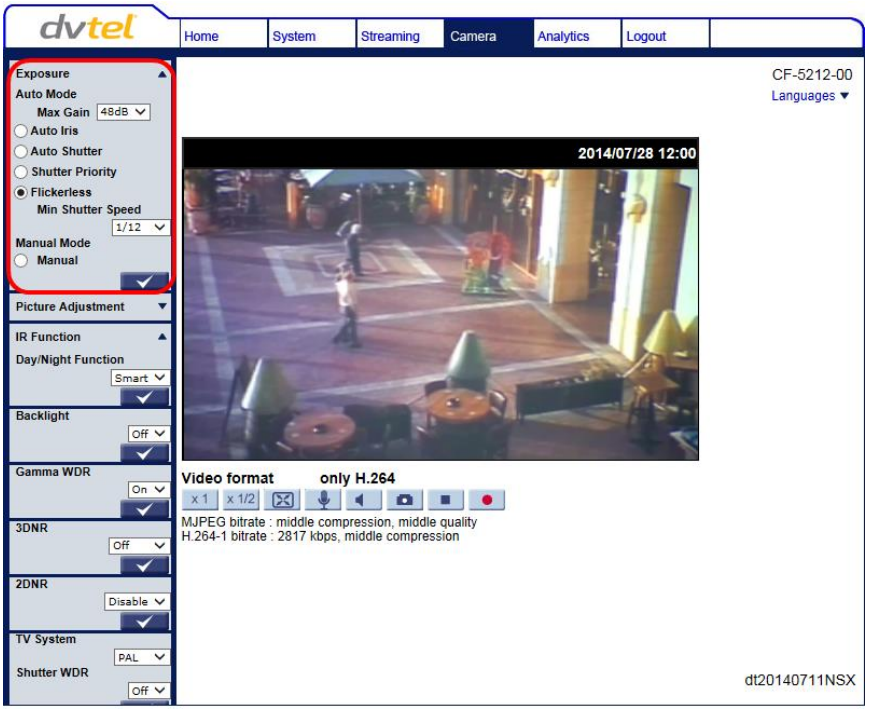


Figure 57: Camera > Exposure Screen

There are two exposure modes: *Auto Mode* and *Manual Mode*.

9.5.2.1.1 Auto Mode

There are five settings within *Auto Mode:*

- *Auto Mode Max Gain* – From the drop-down list, select the maximum gain in 3db steps from *Off* to *72dB*. Increasing the gain lightens dark pictures resulting from low-level lighting. The default setting is *36dB*.
- *Auto Iris Min Shutter Speed* – This mode is recommended to be used in indoor environments involving mixed lighting sources where the main source is fluorescent lighting combined with natural light that enters the scene through windows and other exposed areas. A DC auto iris lens must be used when operating the camera in Auto Iris exposure mode.

  Select this mode to completely open the shutter. The exposure priority is given to the iris. Shutter speed and AGC circuit function automatically in cooperating with the iris to achieve a consistent exposure output.

  The following table displays the shutter speed options. The default setting is *1/12* (PAL) or *1/15* (NTSC).

Auto Iris Min Shutter Speed	
PAL	**NTSC**
1/25	1/30
1/12	1/15

- *Auto Shutter Min Shutter Speed* – This is the default exposure mode of the camera and is recommended for the following scenarios:
  - Outdoor environment
  - Indoor environment with unified lighting (either with constant or changeable lighting conditions) as long as the main light source is fluorescent lighting

  Select this mode so that the camera's shutter speed works automatically to achieve a consistent video output level. You can select a suitable shutter speed according to the environmental luminance.

  The shutter speed range is from *1/12* to *1/425* sec (PAL) to *1/15* to *1/500* sec (NTSC). The default setting is *1/12* (PAL) or *1/15* (NTSC). The following table displays the options.

Auto Shutter Min Shutter Speed	
PAL	**NTSC**
1/425	1/500
1/300	1/350
1/215	1/250
1/150	1/180
1/120	1/125
1/100	1/100
1/75	1/90
1/50	1/60
1/25	1/30
1/12	1/15

- *Shutter Priority* – Select this mode to set a fixed exposure while other parameters can change. The shutter speed range is from *1/25* to *1/425* sec (PAL) to *1/30* to *1/500* sec (NTSC). The default setting is *1/25* (PAL) or *1/30* (NTSC). The following table displays the options.

Shutter Priority	
PAL	**NTSC**
1/425	1/500
1/300	1/350
1/215	1/250
1/150	1/180
1/120	1/125
1/100	1/100
1/75	1/90
1/50	1/60
1/25	1/30

- *Flickerless Min Shutter Speed* – This mode is used to eliminate flicker for indoor applications where fluorescent lighting is used. The darker the ambient lighting, the slower the shutter speed should be. The shutter speed range is from *1/12* to *1/100* sec (PAL) or *1/15* to *1/100* sec (NTSC). The default setting is *1/12* (PAL) or *1/15* (NTSC). The following table displays the options.

Flickerless Min Shutter Speed	
PAL	**NTSC**
1/100	1/100
1/75	1/90
1/50	1/60
1/25	1/30
1/12	1/15

Caution:

Using a slow shutter speed causes moving objects to be blurred.

Attention:

L'utilisation de vitesses d'obturation faibles peut rendre les objets en mouvement flous.

Select <√> to confirm the new setting.

9.5.2.1.2 Manual Mode

This mode should only be used in indoor scenes with consistent lighting. Manual mode requires the user to set fixed values for shutter and gain levels. Increasing the value of the fixed shutter increases the amount of light entering the sensor, which allows a brighter and more detailed image. In a similar manner, utilizing gain and increasing its level increases the sensitivity of the image sensor, which brightens the image and add details. This increases the level of noise in the image.

Caution:

Noise levels can be compromised using the 2DNR/3DNR functions.

Attention:

Les niveaux de bruits peuvent être compromis avec les fonctions 2DNR/3DNR.

Manual Shutter

Select *Manual Shutter* to open the iris completely with a fixed gain. You can select a suitable shutter speed according to the environmental luminance from *1/12* to *1/10000* sec (PAL) or *1/15* to *1/10000* sec (NTSC). The default setting is *1/150* (PAL) or *1/180* (NTSC). The following table displays the options.

Manual Mode - Fixed Shutter Speeds		Manual Mode - Fixed Shutter Speeds	
PAL	**NTSC**	**PAL**	**NTSC**
1/10000	1/10000	1/215	1/250
1/3500	1/4000	1/150	1/180
1/2500	1/3000	1/120	1/125
1/1750	1/2000	1/100	1/100
1/1250	1/1500	1/75	1/90
1/1000	1/1000	1/50	1/60
1/600	1/725	1/25	1/30
1/425	1/500	1/12	1/15
1/300	1/350		

Gain

From the *Gain* drop-down list, select the maximum gain in 3db steps from *Off* to *72dB*. Increasing the gain lightens dark pictures resulting from low-level lighting. The default setting is *Off*. Select <√> to confirm the new setting.

9.5.2.2 Picture Adjustment

The **Picture Adjustment** tab is the same with Shutter WDR enabled or disabled. See Picture Adjustment (page 60).

9.5.2.3 IR Function

The **IR Function** *tab* is the same with Shutter WDR enabled or disabled. See IR Function (page 61).

9.5.2.4 Backlight

In images where a bright light source is behind the subject of interest, the subject would normally appear in silhouette. The backlight function of the camera allows it to adjust the exposure of the entire image to properly expose the subject in the foreground. The default setting *Off*.

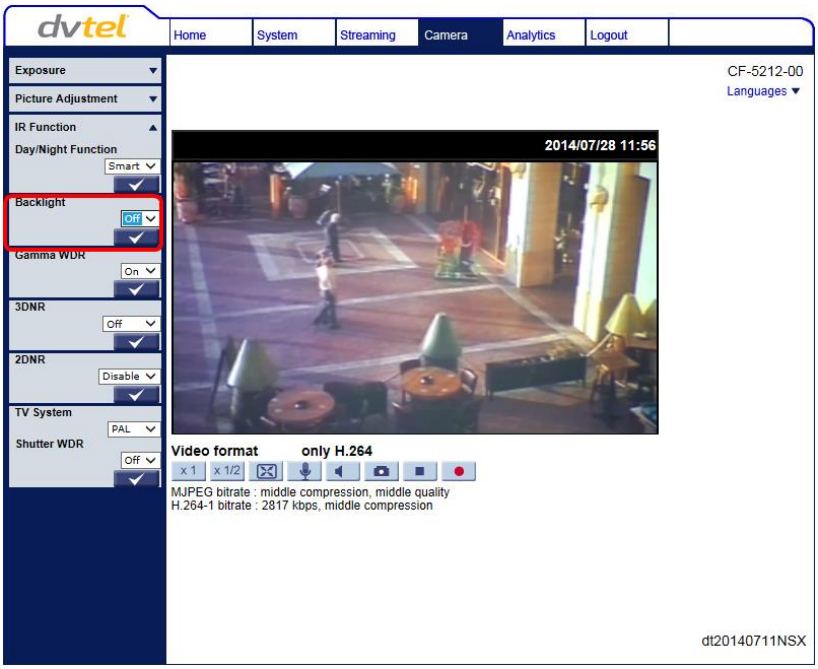


Figure 58: Camera > Backlight Screen

9.5.2.5 Gamma WDR

This function, also known as *Digital WDR,* improves the image quality and amount of details in high contrast scenes. Such scenes combine areas with different lighting conditions, where some areas are very bright and others are dark. If this function was not used, the image either would be overexposed or too bright in bright areas and completely dark in dark areas. Gamma WDR helps to improve image quality by producing a larger amount of details in both the dark and bright areas of the image. The default setting *On*.

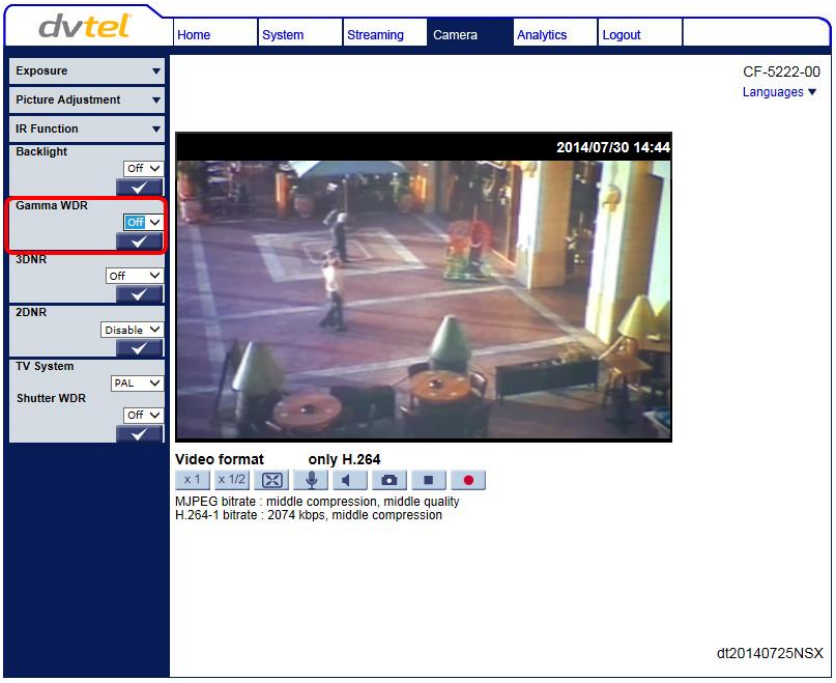


Figure 59: Camera > Gamma WDR Screen

9.5.2.6 3DNR

The **3DNR** tab is the same with Shutter WDR enabled or disabled. See 3DNR (page 62).

9.5.2.7 2DNR

The **2DNR** tab is the same with Shutter WDR enabled or disabled. See 2DNR (page 62).

9.5.2.8 TV System

The **TV System** tab is the same with Shutter WDR enabled or disabled. See TV System (page 63).

9.5.2.9 Shutter WDR

The **Shutter WDR** tab is the same with Shutter WDR enabled or disabled. See Shutter WDR (page 63). Shutter WDR must be set to *Off* in order to display the user interface for the **Camera** tab described in this section. The default setting is *Off*.

Note:

If you select *On* as the *Shutter WDR* setting, the camera restarts automatically and a different user interface is displayed for the **Camera** tab. See section 9.5.1.

9.6 Analytics

The CF-5212/CF-5222 camera includes a rich set of video analytic functionality embedded in its firmware. The **Analytics** tab contains menus for defining the camera's field of view depth and detection rules, including region entrance, loitering, tripwire crossover, fence trespass, unattended baggage, stopped vehicle, and object removal.

In real-time, the camera sends notifications and alarms upon the occurrence of events. You can set customizable rules and criteria to define the perimeter, region, and what to detect. The camera's analytic software ensures a high probability of detection with an extremely low false alarm rate.

Use the **Analytics** tab to configure the following functions:

- Depth
- Rules
- Responses
- Scheduled Actions
- On-Screen Display
- Firmware
- Backup & Restore

Caution:

The camera is disarmed when configuring Analytics. Detection will not take place until the camera is manually re-armed from the **Home** screen.

Attention:

La caméra est désactivée lors de la configuration d'Analytics. La détection n'aura lieu qu'après que la caméra soit réactivée depuis l'écran ***Accueil****.*

9.6.1 Depth

The **Depth** screen enables you define the perspective of the scene being monitored and to. It is used to set human markers, ground guidelines, camera height, horizon, and advanced depth regions (such as hills, planes and fences), which create a virtual 3D model for measurement of distances and sizes from the perspective of the camera. The screen contains a wizard that facilitates configuring the depth settings.

There are two methods to configure depth settings:

- If you are performing setup by yourself, click the *Solo Setup* tab.
- If you are not performing setup alone, proceed to *Step 1: Ground & Height*.

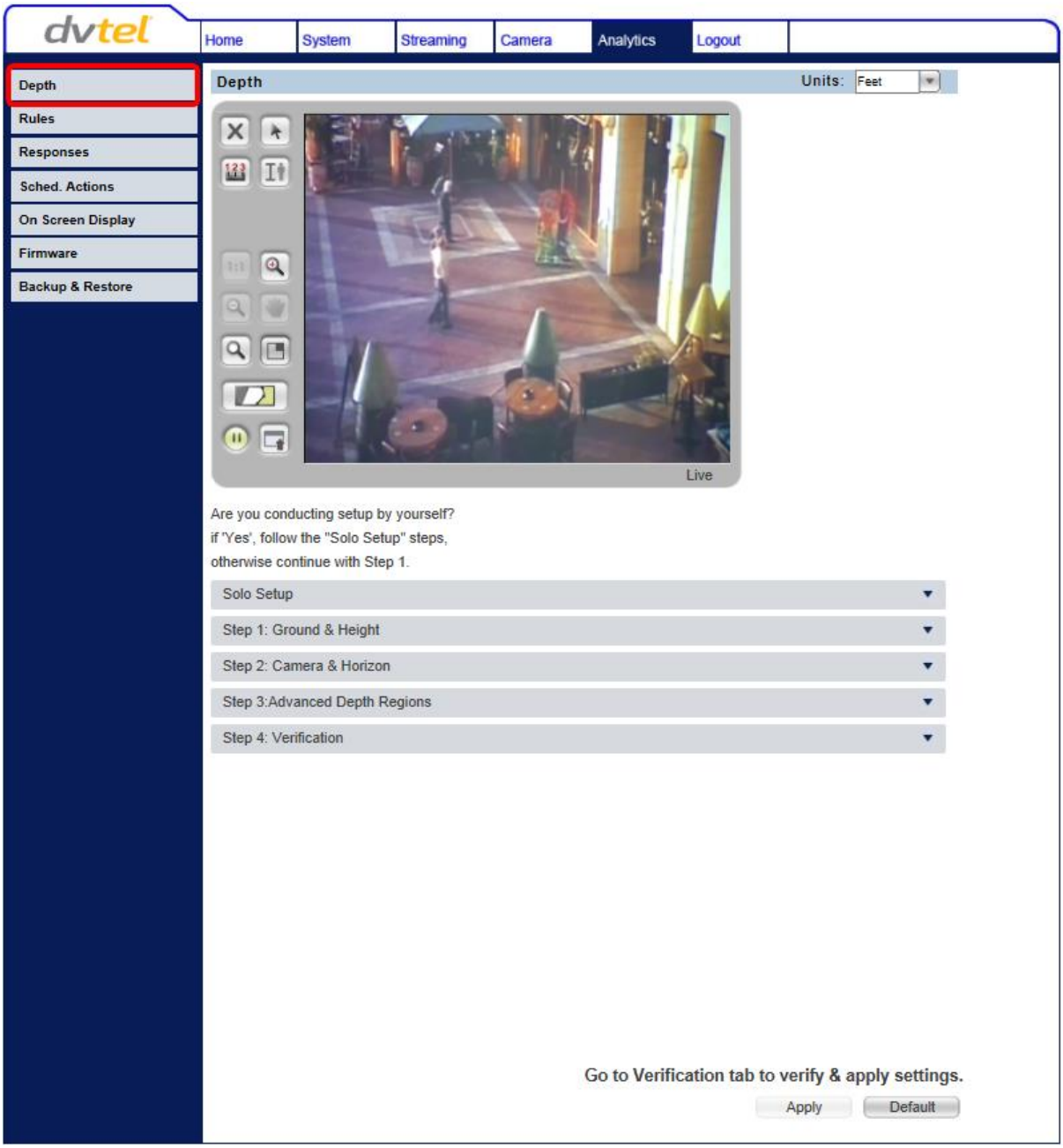


Figure 60: Analytics > Depth Screen

Note:

For detailed instructions how to set markers and guidelines, follow instructions in the *HTML Edition Units User's Guide*.

Note:

It is possible to click the **Verification** tab to verify and apply settings at any time.

9.6.1.1 Solo Setup

The Solo Setup function enables you to install and setup the camera at a remote site without requiring another person's assistance. It is very useful and should be used even if you have another person's assistance.

With this feature, you can:

- Move around within the camera's field of view.
- Use the camera to record a set of snapshots of the scene while the user is moving around the camera field of view. Creating the recording of the person in the FOV can be used to adjust settings without requiring another physical walk through the FOV.
- Use the recording of his movement to setup the depth by marking his height on the camera's field of view.

Follow the instructions in the **Solo Setup** tab to single-handedly setup the camera:

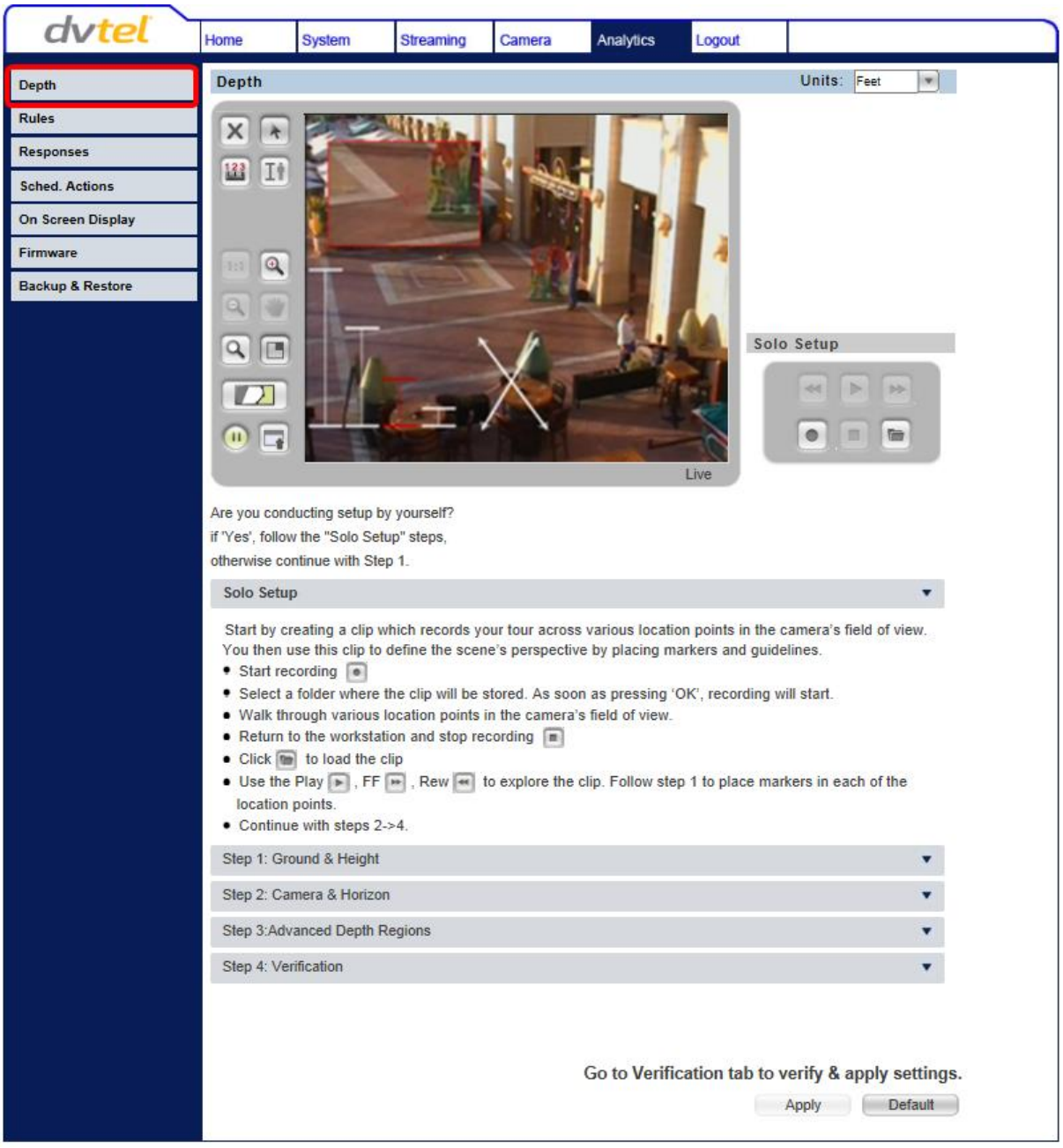


Figure 61: Analytics > Depth > Solo Setup Tab

To perform a solo setup

1. Click the **Solo Setup** tab. The Solo Setup keypad opens with the following control icons:

Icon	Function	Notes
	Start Recording	Starts recording and browses to destination folder where the clip will be saved
	Stop Recording	Stops recording
	Browse	Browses to the destination folder where clip is stored and loads the clip
	Play/Pause	Speed X1/X0
	Fast Forward	Speed X2, X4, X8, X16. Click to increase or decrease speed.
	Rewind	Speed -X2, -X4, -X8, -X16. Click to increase or decrease speed.

2. On the Solo Setup control keypad, click **Start Recording**  to record a view in the camera's field of view.
3. Select a folder where to store the clip. Recording starts when the folder is selected.
4. Walk through various locations across the vertical axis of the camera's field of view in order to place ground and height markers and guidelines in the clip.
5. Click Stop Recording  .
6. Proceed to the tab for **Step 1: Ground & Height**.

> **Note:**
>
> For detailed instructions how to set markers and guidelines, follow instructions in the *HTML Edition Units User's Guide*.

7. Click **Browse** to load the clip from the folder where it is saved.

8. Use the **Play**, **Pause**, **Fast Forward**, and **Rewind** buttons on the Solo Setup keypad to explore the clip. The status of the view is displayed on the bottom left side of the screen.

9. Click the round **Play** button on the control panel located to the left of the monitor to exit *Clip* mode and return to *Live* mode. The caption under the monitor changes from *Clip* to *Live.*

Figure 62: Analytics > Depth Control Panel

10. Repeat steps 3-9 above for each preset.

11. Proceed to the tabs for Steps 2-4 of the Depth Setup to complete the setup and apply settings.

> **Note:**
>
> At any time it is possible to click the **Verification** tab to verify and apply settings.

9.6.1.2 Configuring Ground and Height Settings

If you are not performing a solo setup, click the **Step 1: Ground & Height** tab.

To configure ground and height settings

1. Click the Step 1: Ground & Height tab.

2. Follow the instructions on screen.

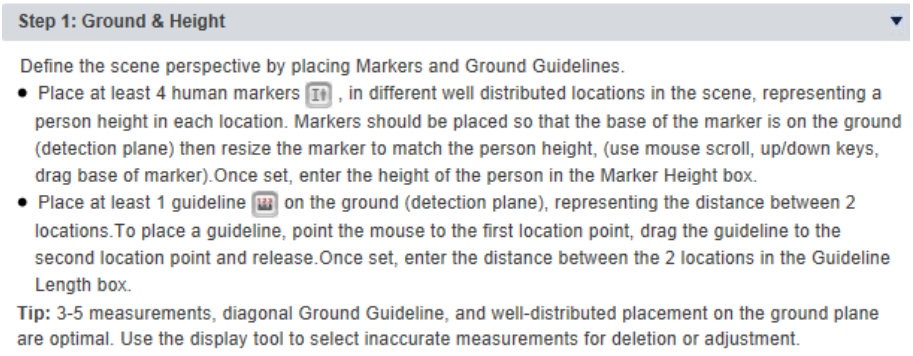


Figure 63: Analytics > Depth > Step 1: Ground & Height Tab

3. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.
4. Click **Apply** when finished or continue to the next step.

9.6.1.3 Configuring Camera and Horizon Settings

After completing Solo Setup or configuring ground and height settings, configure camera and horizon settings.

To configure camera and horizon settings

1. Click the Step 2: Camera & Horizon tab.
2. Follow the on-screen instructions to configure camera and horizon settings.

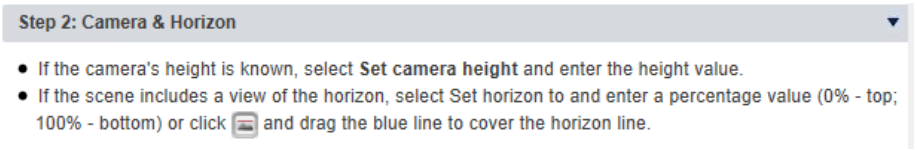


Figure 64: Analytics > Depth > Step 2: Camera & Horizon Tab

3. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.
4. Click **Apply** when finished or continue to the next step.

9.6.1.4 Configuring Advanced Depth Region Settings

After configuring camera and horizon settings, configure advanced depth region settings.

To configure advanced depth region settings

1. Click the Step 3: Advanced Depth Regions tab.
2. Follow the on-screen instructions to configure advanced depth region settings.

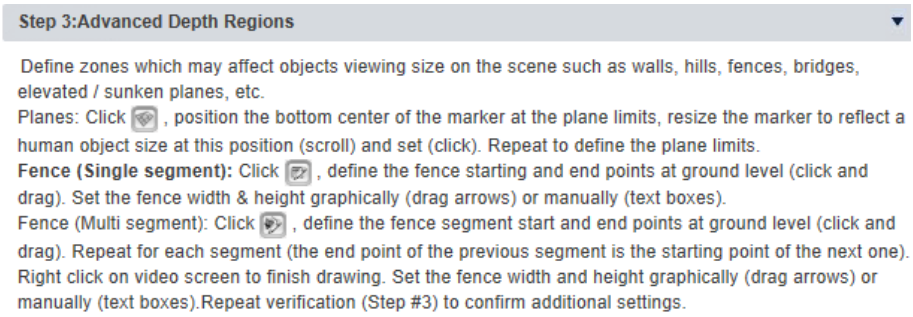


Figure 65: Analytics > Depth > Step 3: Advanced Depth Regions Tab

3. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.
4. Click **Apply** when finished or continue to the next step.

9.6.1.5 Verification of Settings

After configuring advanced depth region settings, verify your settings.

To verify settings

1. Click the Step 4: Verification tab.
2. Follow the on-screen instructions to verify settings.

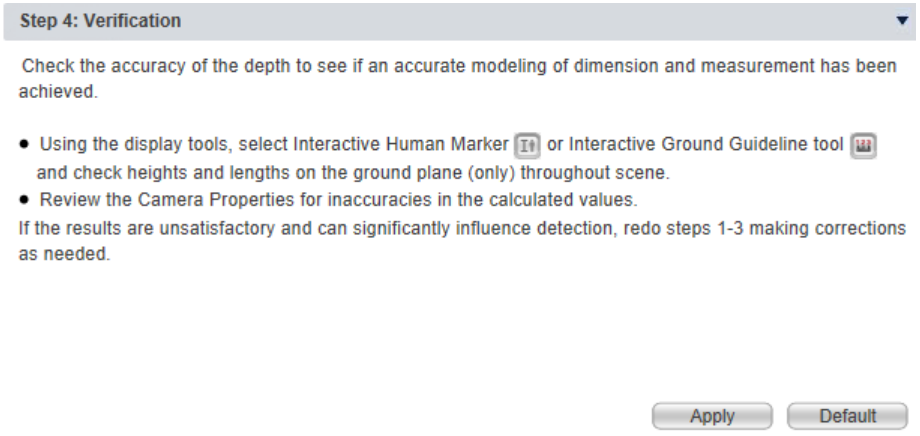


Figure 66: Analytics > Depth > Step 4: Verification Tab

3. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.
4. Click **Apply** when finished.

9.6.2 Rules

The **Rules** tab enables you to define detection rules according to the type of detection you want to be notified about. By default, the *Human or vehicle enter region* rule is enabled.

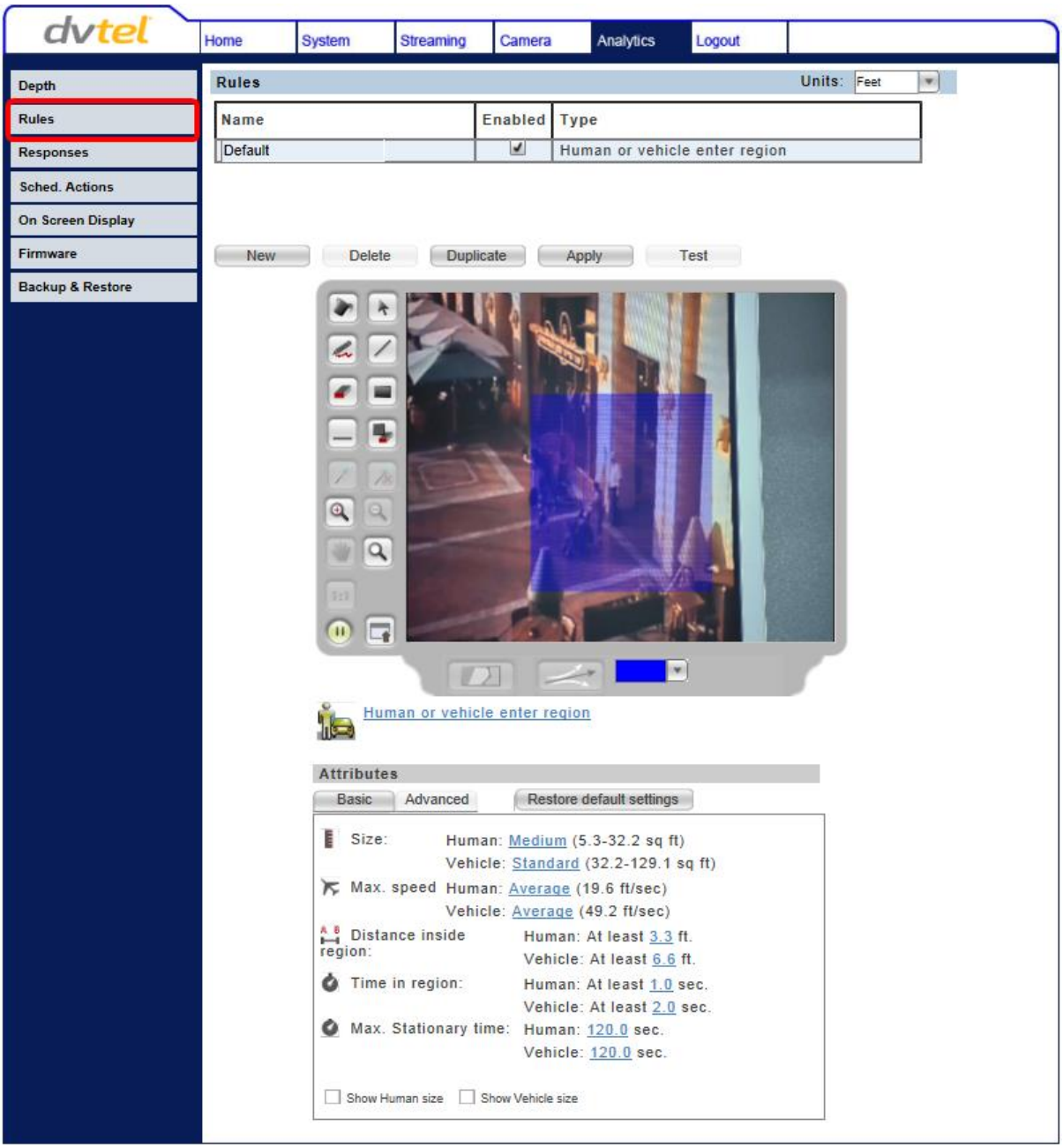


Figure 67: Analytics > Rules Screen

Detection occurs when one or more detection rules are active, the camera is in *Arm* mode, and the scenario on the video (scene) fits the detection criterion specified. When the conditions of a detection rule are met, an alarm is shown in which you can observe the detection and take the appropriate action.

Rules are selected by clicking the **Attributes** tab. The *Basic* tab displays minimal information for the rule.

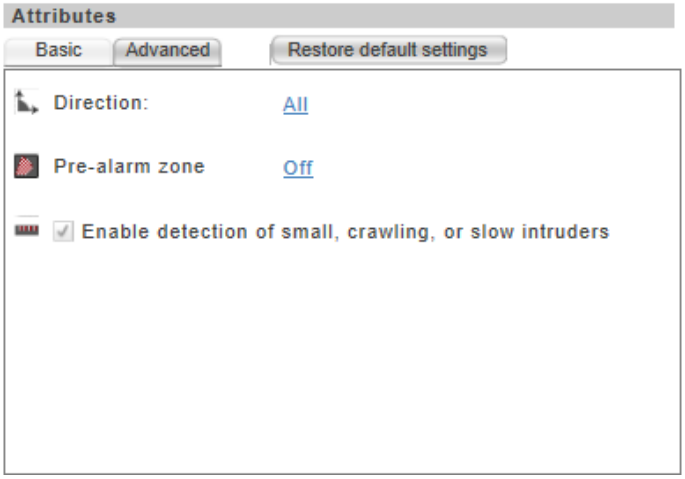


Figure 68: Analytics > Rules > Basic Attributes Tab

The *Advanced* tab displays additional information for the rule.

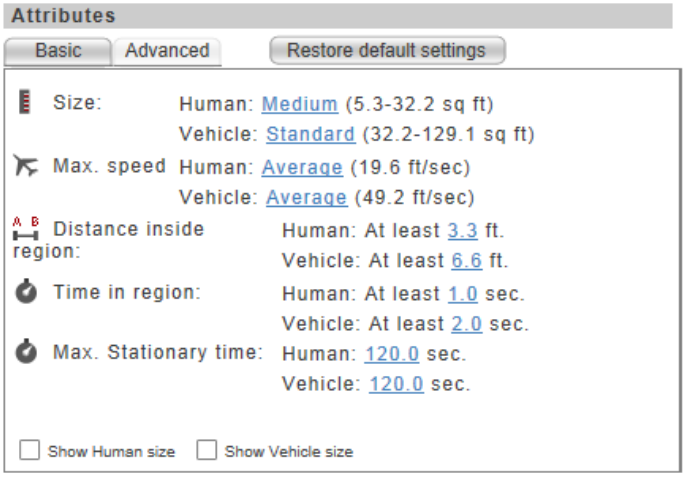


Figure 69: Analytics > Rules > Advanced Attributes Tab

Click *Restore default settings* to return to factory default settings.

Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

9.6.3 Responses

The camera's embedded event engine enables you to define a set of responses (automatic actions) for selected events and to perform actions (scheduled actions) at pre-defined times during a defined monitoring period. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

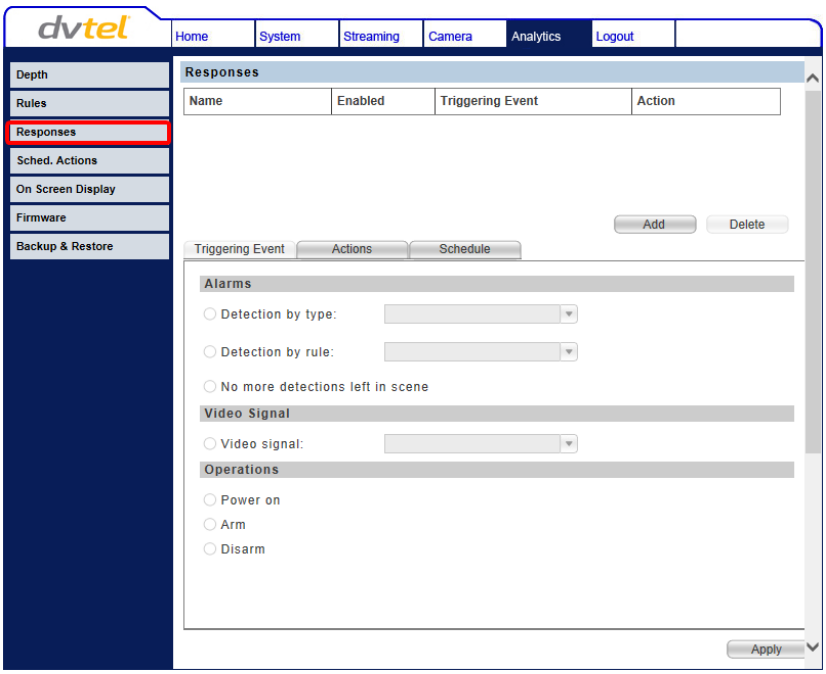


Figure 70: Analytics > Responses Screen

Each automatic response definition includes the following three parameters:

- Triggering event – The event that will start the automatic response.

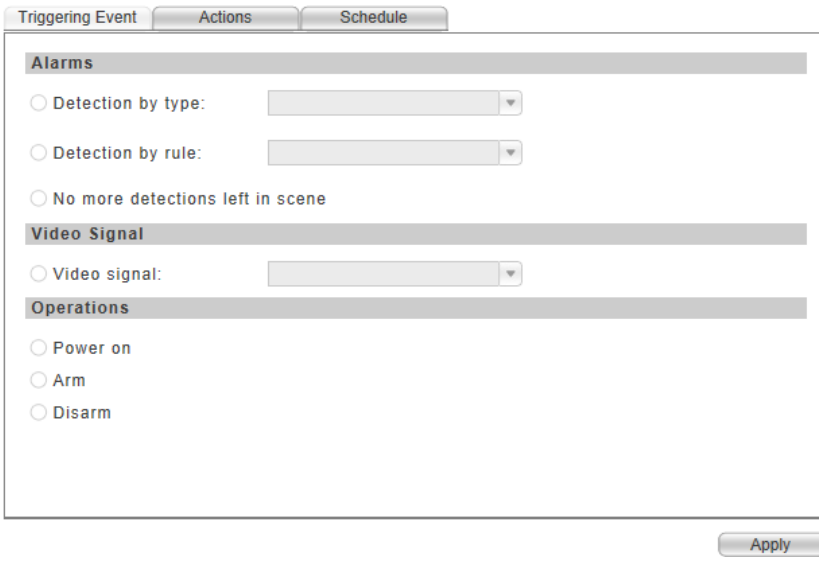


Figure 71: Triggering Event Tab

- Actions – The actions to perform in response to the occurrence of the triggering event.

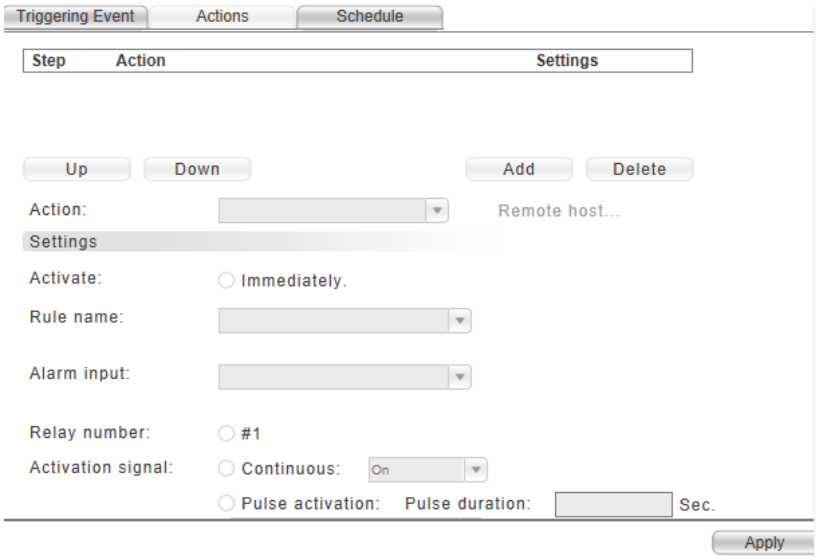


Figure 72: Actions Tab

- Schedule – When to monitor for the triggering event occurrence.

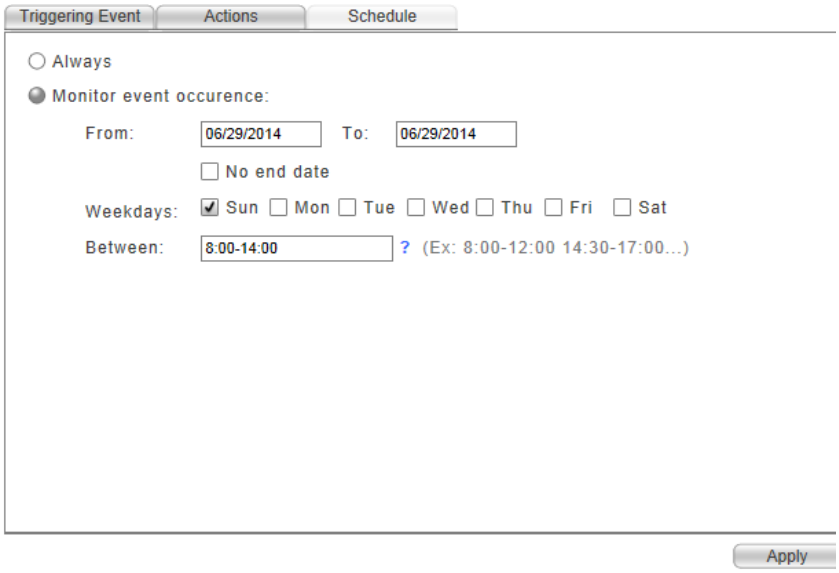


Figure 73: Schedule Tab

9.6.4 Scheduled Actions (Sched. Actions Screen)

The **Responses** and **Sched. Actions** screens are similar, except that the **Sched. Actions** screen does not include the *Triggering Event* tab. See section 9.6.3, Responses.

Each scheduled action includes the following two parameters:

- Actions – The actions to perform at the scheduled time.
- Schedule – When the actions must be performed.

Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

9.6.5 On Screen Display

The **On Screen Display** screen determines the information to be displayed on the video screen as an overlay on top of the video. The settings on this screen define the selection, alignment and color configuration of the various overlays that appear during normal monitoring, events and detection.

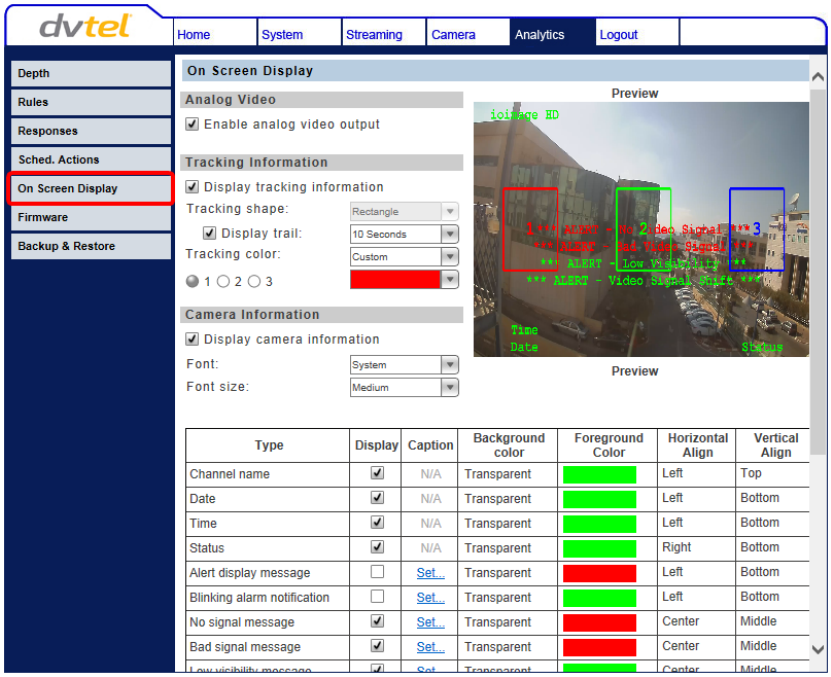


Figure 74: Analytics > On Screen Display Screen

The **On Screen Display** screen includes the following default settings:

- Enable analog video output
- Display tracking information
- Tracking shape: Rectangle
- Display trail enabled (10 seconds)
- Tracking color: Custom
- Radial button 1: Red
- Display camera information
- Font: Terminal
- Font size: Medium

In the table, select the settings that you want to configure.

- In the *Display* column, select the checkbox to display the display item.
- In the *Caption* column, click *Set* to change the name of the display item. You cannot change the names *Channel name, Date, Time* and *Status*.
- In the *Background color, Foreground color, Horizontal Align,* and *Vertical Align* columns, clicking a field opens a drop-down list. Select one of the options from the drop-down list.

Click **Apply** when finished.

Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

9.6.6 Firmware

The **Firmware** screen displays the current firmware version and enables you to update the unit's analytics firmware version. To search for the analytics firmware file, click **Browse**, select the file, then click **Upgrade**.

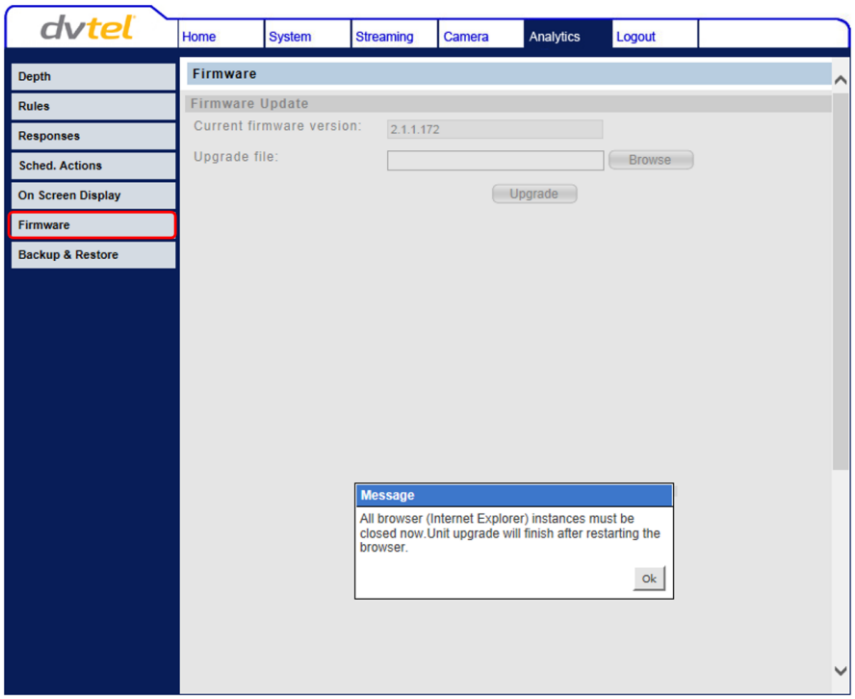


Figure 75: Analytics > Firmware Screen

In the *Advanced Settings* area, *Scene with large objects or many objects* and *Enable enhanced detection* are enabled by default.

Click **Apply** when finished.

Note:

Analytics firmware is stored in a separate file than the camera system software. To view the camera system software version, see System > Software Version. To upgrade the camera system software version, see System > Software Upgrade.

Note:

You must close and restart Internet Explorer in order to view the new firmware version.

Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

9.6.7 Backup & Restore

The **Backup & Restore** screen enables you to create backup files of the unit's analytics settings and to restore them.

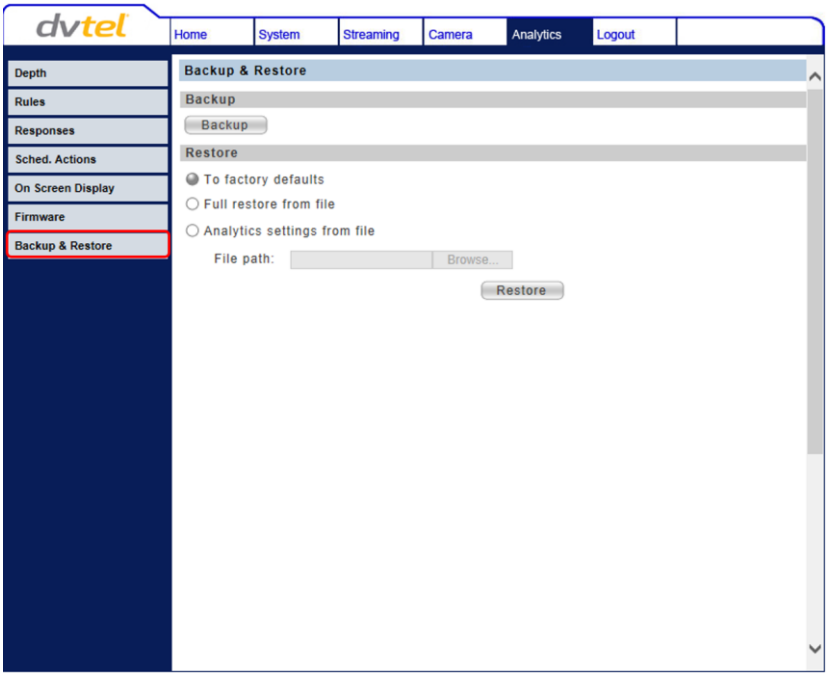


Figure 76: Analytics > Backup & Restore Screen

To back up the analytic firmware file

- Click **Backup**.

To restore the analytic firmware file

- Do one of the following:
  - To restore factory defaults, select *To factory defaults.*
  - To restore all defaults from a stored file, select *Full restore from file,* click **Browse** to locate the file path, then select the file.
  - To restore analytic settings from a stored file, select *Analytic settings from file,* click **Browse** to locate the file path, then select the file.
- Click **Restore**.

Note:

Analytics firmware is stored in a separate file than the camera system software. To backup and restore the camera system software version, see System > Factory Default.

Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

9.7 Logout

Selecting the **Logout** tab in the navigation bar closes the session. The following message appears:

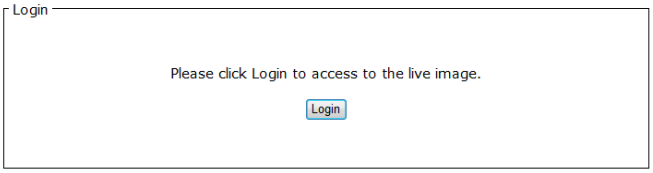


Figure 77: Login Message

Upon clicking **Login,** the **Login** window opens.

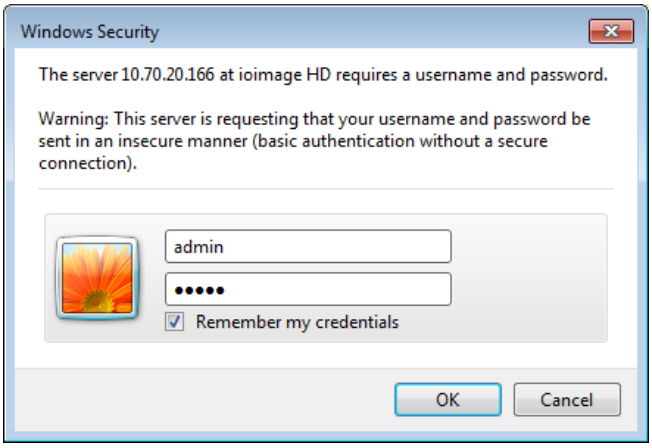


Figure 78: Login Window

Appendices

A.1. Technical Specifications

Camera		**CF-5212**	**CF-5222**
Image Sensor		1/3” Progressive 1.3MP CMOS	1/2.8” Progressive 2.1MP CMOS
Effective Pixels (H x V)		1280 x 1024	1920 x 1080
Video Resolution		HD 720p	Full HD 1080p
Shutter Speed	PAL	1/1.5 to 1/10,000 with 18 options	
	NTSC	1 to 1/10,000 with 19 options	
Sensitivity (w/ analytics)	Color Mode	0.1 lux @ F1.4 @ 15 FPS, 36dB max. gain	0.2 lux @ F1.4@ 15 FPS, 36dB max. gain
	Night Mode	0.05 lux @ F1.4 @ 15 FPS, 36dB max. gain	0.1 lux @ F1.4@ 15 FPS, 36dB max. gain
Enclosure		Tamper-resistant surface mount plastic case or IK10 rated vandal IP66	
Lens			
Lens Type		See Mounting and Lens Accessories for a list of optional lenses.	
Lens Mounting		CS mount	
Video			
Video Resolution	H.264	HD 720p/D1	Full HD 1080p/HD 720p/D1
	MJPEG	HD 720p/D1	Full HD 1080p/HD 720p/D1
Video Streaming		Single stream H.264 720p (25/30fps) or MJPEG 720p (25/30fps)	Single stream H.264 1080p (25/30fps) or MJPEG 1080p (25/30fps)
Video Compression		Fully compliant H.264 main profile/MJPEG	
Maximum Performance		60fps @ HD 720p	45fps@ Full HD 1080p

Operation			
Image Settings	Exposure	With Shutter WDR Enabled	With Shutter WDR Disabled
		Auto Mode	DC Auto Iris/Auto Shutter/ Shutter Priority/Flickerless/ Manual Mode
	Brightness	Manual	
	Sharpness	Manual (3 levels)	
	Contrast	Manual (3 levels)	
	Saturation	Manual (15 levels)	
	Hue	Manual (15 levels)	
	Removable IR Cut Filter	Auto/Day/Night/Smart	
	Backlight Compensation	With Shutter WDR Enabled	With Shutter WDR Disabled
		N/A	On/Off
	Digital (Gamma) WDR	With Shutter WDR Enabled	With Shutter WDR Disabled
		N/A	On/Off
	3D Noise Reduction	On/Off + 3 levels	
	2D Noise Reduction	On/Off + 3 levels	
	Wide Dynamic Range (WDR)	On/Off	
Audio	Bi-Directional Audio	Line-out Line-in/Mic-in	
	Audio Compression	G.711/G.726 (not supported by Latitude)	
	Audio Connections	Terminal block	
Alarm	Input	5V 10kΩ pull up	
	Output	Photo relay output 300VDC/AC	
Event Notification		FTP, SMTP, HTTP	
Languages		English, German, Spanish, French, Italian, Japanese, Korean, Portuguese, Russian, Simplified Chinese, and Traditional Chinese	
MicroSD Card Recording		This function is not supported in the current version and is not supported by Latitude.	

Network		
Interface		10/100Mbps Ethernet (RJ45)
Network Protocols		IPv4, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, NTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, and ONVIF™ Profile S
Password Levels		User and Administrator
Security		HTTPS, IP Filter, IEEE 802.1x
Operating System		Windows XP, 7, 8, 8.1
Internet Browser		Internet Explorer 9, 10, 11
User Accounts		20
Mechanical		
Connectors	Power	3-pin terminal block
	Ethernet/PoE	RJ45
	Audio	Line-out: 3.5 mm audio jack Line-in/Mic-in: 3.5 mm audio jack
	Alarm	7-pin terminal block with 2-pin alarm input and 2-pin relay output
	Analog Video	1.0V p-p, 75Ω BNC connector
	MicroSD card	Not supported
LED Indicator		Power, Link, ACT
Dimensions (L x W x H)		125 x 82 x 52 mm (4.9 x 3.2 x 2 in.) without lens
Weight		330g (0.73 lbs.)
Electrical		
Power Source		12VDC/24VAC/PoE (802.3af Class 0)
Power Consumption		8W
Power Connector		AC/DC/PoE
Environmental		
Operating Temperature		-10° to 50° C (-14° to 122°F)
Humidity		10-90% non-condensing
General		
Regulatory	US	FCC (47 CFR) Part 15, Subpart B, Class A; UL
	International	CE-marked (IEC 60950-1:2005+A1:2009 and EN 60950-1:2006+A11:2009+A1:2010+A12:2011); EN55022:2010/AC:2011 (Class A); EN55024, IEC 61000; EN61000; CISPR 22: 2009 Class A; EN 50130; ICES-003 Issue 5; RoHS
Warranty		No less than 4 years from purchase date

A.2. Internet Security Settings

If ActiveX control installation is blocked, either set Internet security level to default or change ActiveX controls and plug-in settings.

Internet Security Level: Default

1. Start Internet Explorer (IE).
2. From the Command Bar toolbar, select **Tools** and select **Internet Options** from the menu that appears.

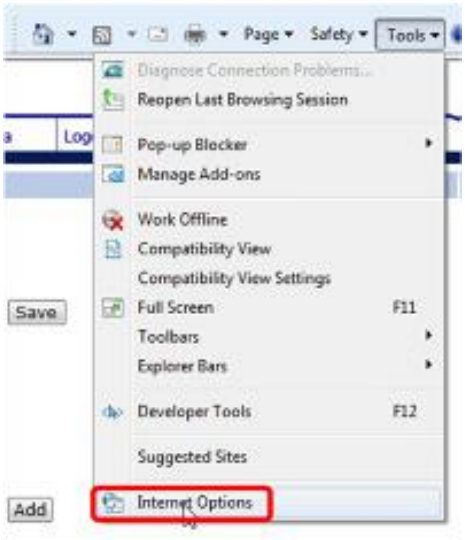


Figure 79: Command Bar Toolbar – Select Internet Options

3. In the **Internet Options** window that appears, select the **Security** tab.
4. Select 

in Select a zone to view or change security settings.
5. If the settings are not defined as default, select **Default Level** and move the Allowed levels for this zone slider to Medium-high and select **OK**.

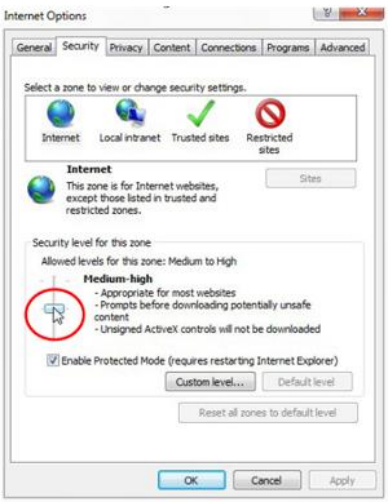


Figure 80: Internet Options Screen

6. Close all browsers and reopen so that the settings take effect.

ActiveX Controls and Plug-in Settings - Creating a Custom Level

1. Start Internet Explorer (IE).
2. From the Command Bar toolbar, select **Tools** and select **Internet Options** from the menu that appears.

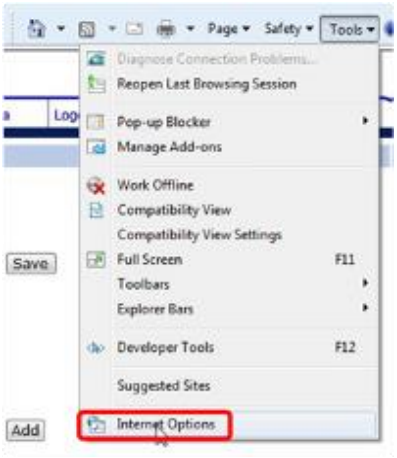


Figure 81: Command Bar Toolbar – Internet Options

3. In the Internet Options window that appears, select the **Security** tab.
4. If not already selected, select 

, then select *Custom Level*.
5. In the dialog that appears, under **ActiveX controls and plug-ins** set ALL the following options (listed below) to **Enable** or **Prompt**:
   - Automatic prompting for ActiveX controls
   - Binary and script behaviors
   - Download signed ActiveX controls
   - Download using ActiveX controls
   - Initialize and script ActiveX not marked as safe
   - Run ActiveX controls and plug-ins
   - Script ActiveX controls marked safe for scripting

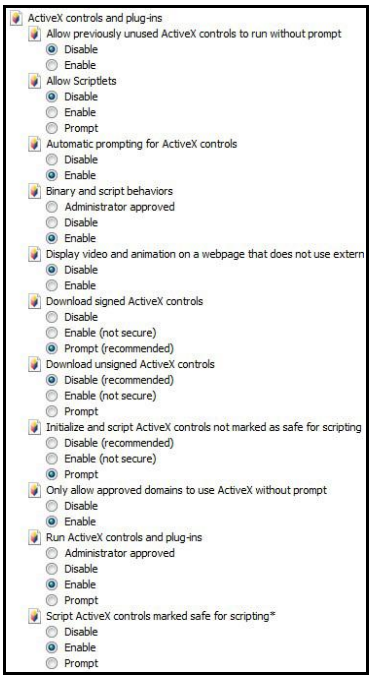
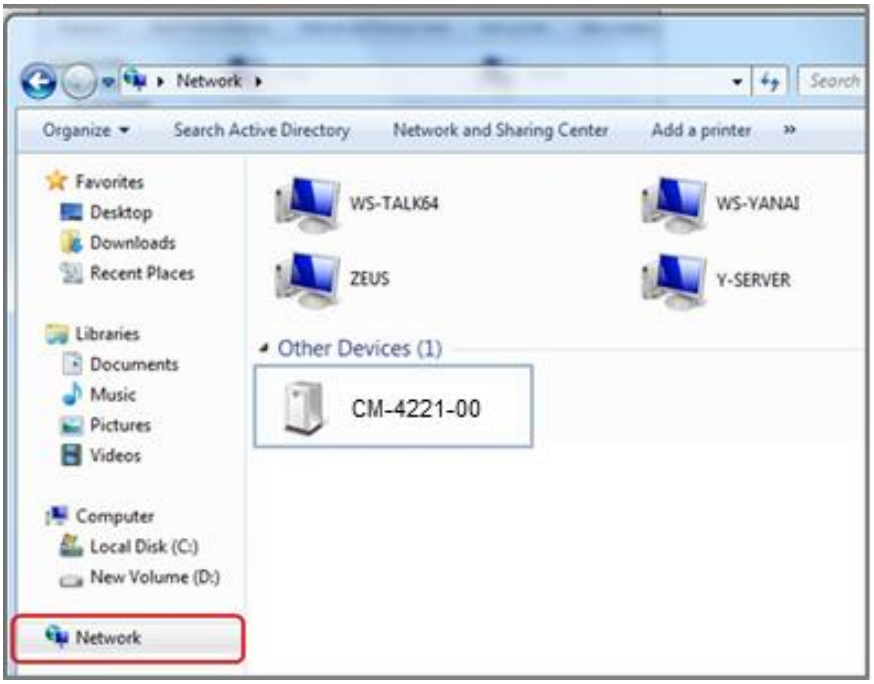


Figure 82: Schedule Screen

6. Click **OK** to accept the settings and close the **Security** screen.
7. Click **OK** to close the **Internet Options** screen.
8. Close the browser window and restart IE again to access the camera.

A.3. Install UPnP Components

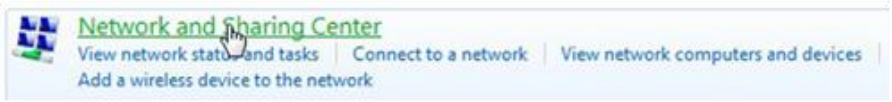
Follow the instructions below to enable UPnP so that the camera can be discovered and displayed in Network locations under *Other Devices*:



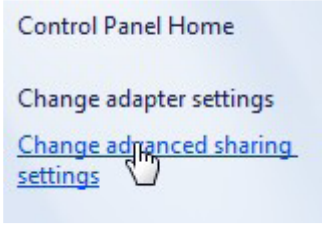
To enable UPnP discovery in Windows 7, Windows 8, and Windows 8.1

1. Click (Start) and select *Control Panel*.
2. Click on Network and Internet.

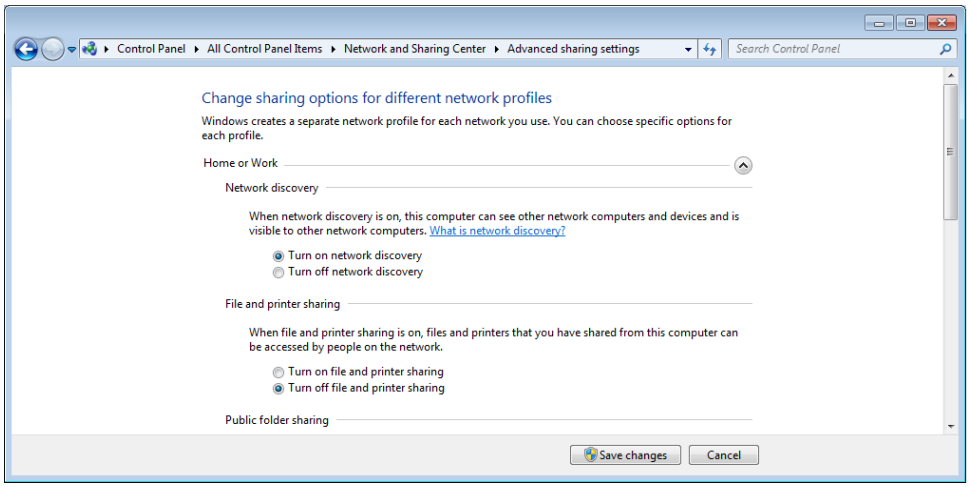
3. Click on Network and Sharing Center.



4. Click Change advanced sharing settings.



5. Expand the Home or Work node, select *Turn on network discovery.*

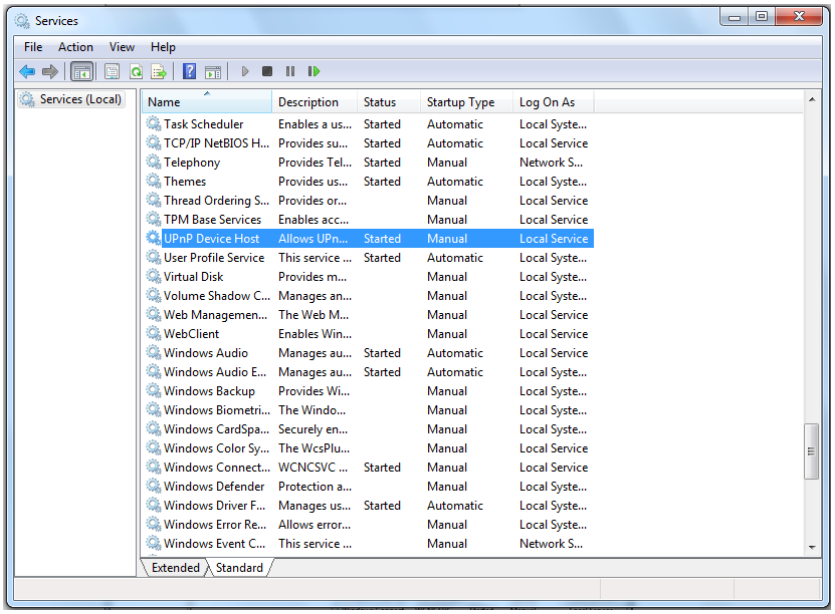


6. Click Save Changes.

> **Note:**
>
> Network discovery requires that the DNS Client, Function Discovery Resource Publication, SSDP Discovery, and UPnP Device Host services are started, that network discovery is allowed to communicate through Windows Firewall, and that other firewalls are not interfering with network discovery.

To check that the UPnP Device Host services are running

1. Click  (Start) and type in the Search programs and files field **services.msc.**
2. Select **services.msc** from the displayed Programs. The **Services** dialog box appears.



3. In the **Services** dialog box, scroll down the list to *UPnP Device Host* and verify that it shows the status *Started*. If *Started* is not displayed, right-click and select **Start** from the shortcut menu.

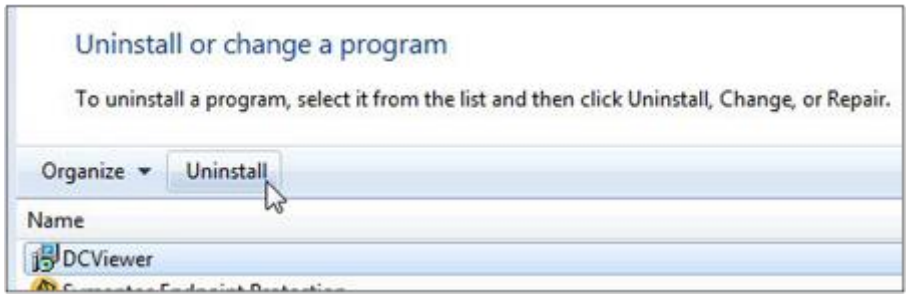
A.4. Deleting the Existing DCViewer

Users who have previously installed the DCViewer in the PC should first delete the existing DCViewer from the PC before accessing the camera.

To delete a legacy DCViewer

1. Click **Start** and select *Control Panel*.
2. In the Control Panel, click **Uninstall a program**.

3. From the installed program list, select **DCViewer** and then, on the banner bar, click **Uninstall**.



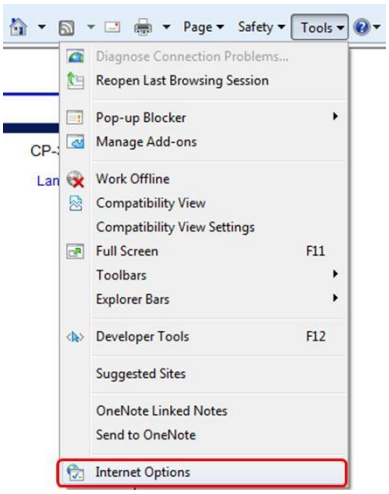
4. If prompted to confirm the uninstall, click **Yes**.

A.5. Deleting Temporary Internet Files

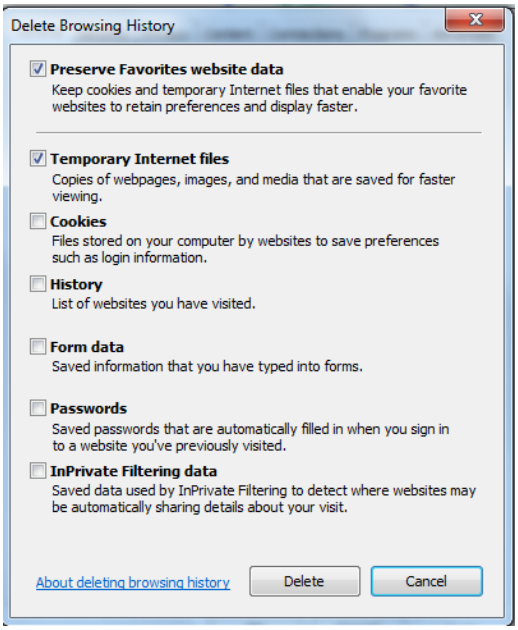
To improve browser performance, it is recommended to clean up all of the Temporary Internet Files. The procedure is as follows:

To delete temporary Internet files

1. In Internet Explorer (IE), from the Command Bar toolbar, click **Tools** and select *Internet Options* from the menu that appears.



2. In the General tab in the **Internet Options** dialog box, click **Delete**.
3. In the **Delete Browser History** dialog box that appears, select *Temporary Internet files*. Deselect *Cookies and History* to keep this data. Then click **Delete**.



A.6. Back Focus Adjustment

When to adjust back focus

Back focus refers to the distance from the rear lens element to the camera focal plane. In most cases, it is required to adjust back focus only when the camera's lens cannot hold focus throughout its zoom range. If the focus cannot be achieved within the zoom range, you may need to adjust the back focus.

Requirements:

Tools required when carrying out back focus adjustment include:

- Back focus adjuster (in the IP camera's package)
- Test chart/contrasting object

To adjust back focus

1. Set the Exposure Settings as follows:
   - **a.** In the Viewer, select the **Camera** tab.
   - **b.** From the **Exposure** menu, select *Auto Shutter mode*. See Camera-Related Settings.
2. Do the following:
   - **a.** View an object at least 75 feet (23 meters) away. For greater telephoto capable lenses, the object can be located further away. If the field of view is less than this distance, the object should be as distant as possible.
   - **b.** Adjust the zoom to the extreme telephoto position.
   - **c.** Adjust the focus to the best possible focused image.
   - **d.** If the image is not focused (sharp), loosen the back focus ring retaining screw with the supplied hex tool and rotate the lens mount to adjust the back focus as needed to achieve a sharp picture in focus.

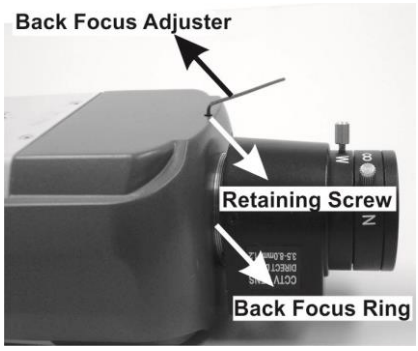


Figure 83: Back Focus Adjustment

   - **e.** Zoom out to wide-angle position (for close FOV) and attempt to focus on a close object (e.g. 1-3m.).
   - **f.** Repeat steps a. through e. until focus is optimal throughout the zoom range.
   - **g.** Tighten the back focus ring retaining screw to secure the ring in place.
   - **h.** Return the camera's Exposure Setting to *Auto Iris* if this was temporarily changed to *Auto Shutter* mode during focusing.

A.7. Connecting Wires to a Spring Clamp Terminal Block

The unit is delivered with a 7-terminal I/O block and a 3-terminal power connection block. The terminal blocks enable you to connect wires to the unit.

Figure 84: Typical Spring Clamp Terminal Block

To connect a wire to the spring clamp terminal block

1. Strip the insulation from the end of each wire that is to be connected to the terminal block. Approximately 1 cm (2.54”) of wire should be exposed.
2. With a small screwdriver, press in and hold the orange spring clamp button next to the female outlet where the wire will be inserted.
3. Insert the stripped end of the wire into the female outlet.
4. Release the orange spring clamp button.

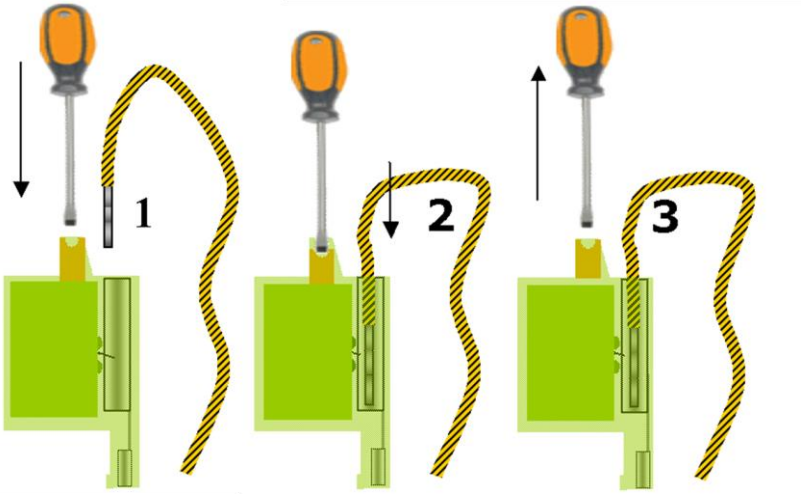


Figure 85: Connecting a Wire to a Terminal Block

A.8. Mounting and Lens Accessories

The following mounting accessories are available from DVTEL for installation of your ioimage HD CF-5212 and CF-5222 series compact fixed IP cameras. For more information on available options, contact your DVTEL sales representative or visit www.DVTEL.com to request details on where to get the accessories you need.

Image	Name	Description
	**Mounting Accessories**	
	CF-X200-01	Outdoor fixed camera housing: • Equipped with heater and fan • 24VAC @ 20W • Aluminum with sunshield • -30 to +50C (-22 to +122F) • 140 x 112x 340mm/ 5.5 x 4.4 x 13.4” (W x H x L) • 1.51Kg/3.4 lbs. • Mounting bracket, screws and wrenches
	CF-X200-POLE	Pole Mount Option for CF-X200-01 Housing
	**Lenses**	
	CF-L131-08-50	8-50mm, f1.6, 1/2.7”, 5MP Auto Iris, IR Corrected, CS-Mount
	CF-L131-31	3.1-8mm, f1.2, 1/2.7”, 5MP Auto Iris, IR Corrected, CS-Mount
	CF-L131-08	8-80mm, f1.4, 1/2”, 5MP Auto Iris, IR Corrected, C-Mount, packaged with CS adapter
	CF-L131-12	12.5-50mm, f1.4, 1/2.7”, 5MP Auto Iris, IR Corrected, CS-Mount

Contacting DVTEL

DVTEL Inc. is a multiple award-winning market leader in the development and delivery of intelligent security solutions over IP networks. DVTEL provides unified solutions that leverage existing network infrastructure, while providing unmatched levels of flexibility, scalability and cost-effectiveness - all backed by superior customer support.

To contact us, write us at info@dvtel.com, or contact your local office.

CORPORATE HEADQUARTERS **DVTEL, Inc.** 65 Challenger Road Ridgefield Park, NJ 07660 USA Tel: +1 201.368.9700 Fax: +1 201.368.2615 info@dvtel.com	**ASIA PACIFIC REGION** **DVTEL** 111 North Bridge Road, #27-01 Peninsula Plaza Singapore 179098 Tel: +65 6389 1815 Fax: +65 6491 5660 info.apac@dvtel.com
ANZ AND THE PACIFIC ISLANDS **DVTEL** 37 Victoria Street Henley Beach, SA 5022 Australia Tel: +61 8 8235 9211 Fax: +61 8 8235 9255 info.anz@dvtel.com	**EMEA** **DVTEL UK Ltd.** 7 Lancaster Court Coronation Road High Wycombe HP12 3TD England Tel: +44 (0) 1494 430240 Fax: +44 (0) 1494 446928 info.uk@dvtel.com
INDIA AND SAARC, GULF REGION **DVTEL, India Pvt., Ltd** 303 SSR Corporate Park Mathura Road Faridabad 121002 Haryana, India Tel: +91 (129) 431 5031 Fax: +91 (129) 431 5033 info.asia@dvtel.com	**CENTRAL AND LATIN AMERICA** **DVTEL Mexico S.A.P.I. de C.V**. Felipe Villanueva No. 10 Col. Guadalupe Inn México, D. F. 01020 México Tel: +52 55 5580 5618 Fax: +52 55 8503 4299 info.cala@dvtel.com
DVTEL NORTH ASIA 2404, 24/F, World-Wide House 19 Des Voeux Road Central Hong Kong Tel: +852 3667 9295 Mobile: +852 9479 4195 info.northasia@DVTEL.com	**DVTEL**北亞地區 **香港中環德輔道中19號** **環球大廈2404室** **電話**: +852 3667 9295 手提: +852 9479 4195 電郵: info.northasia@dvtel.com

To request the latest versions of firmware and software or to download other product-related documents, visit http://www.dvtel.com/support. If you have obtained a login, go to our support gateway. For assistance, e-mail us at support@dvtel.com or phone 1-888-DVTEL77.